(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002041482 A**

(43) Date of publication of application: **08.02.02**

(51) Int. Cl **G06F 15/00**
G09C 1/00
H04L 9/08
H04L 9/10
H04L 9/32
H04N 5/85
H04N 5/91
H04N 7/167

(21) Application number: **2000220720**

(22) Date of filing: **21.07.00**

(71) Applicant: **HITACHI LTD SEGA CORP**

(72) Inventor: **NISHIOKA GENJI**
SETO YOICHI
WAKABAYASHI TAKASHI
TETSUI TOSHIAKI
YAMANAKA ISATAKE

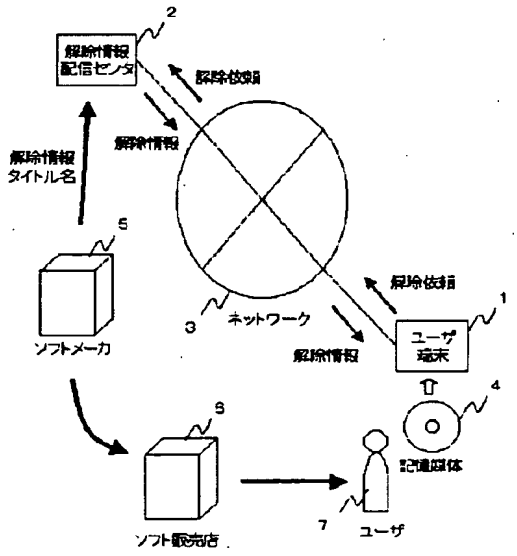
(54) **METHOD FOR RELEASING CONTENTS UTILIZATION LIMITATION AND STORAGE MEDIUM**

(57) Abstract:

PROBLEM TO BE SOLVED: To evaluate contents in advance of the formal purchase of the contents, without imposing excessive load on a user.

SOLUTION: The contents the utilization of a part of which is limited by some method are stored together with a utilization limitation release program in a storage medium 4 and offered to the user. The user inserts the purchased storage medium 4 into a user terminal 1 and can actually try available part of the contents. When the user likes the part, the user starts the utilization limitation release program, transmits a release request which includes the title name of the contents to a release information distribution center 2 via a network 3 and can purchase the release information of the contents. The utilization limitation of the contents can be released by the utilization limitation release program.

図1



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－41482
（P2002－41482A）
(43)公開日　平成14年２月８日(2002.2.8)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
G06F	15/00	330	G06F	15/00	330Z　5B085
G09C	1/00	660	G09C	1/00	660A　5C052
H04L	9/08		H04N	5/85	Z　5C053
	9/10		H04L	9/00	601A　5C064
	9/32				601E　5J104

審査請求　未請求　請求項の数21　ＯＬ　（全 30 頁）　最終頁に続く

(21)出願番号　特願2000－220720(P2000－220720)

(22)出願日　平成12年７月21日(2000.7.21)

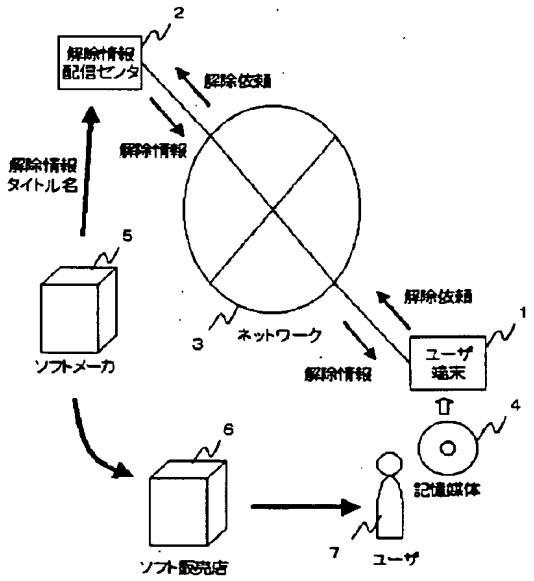
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(71)出願人　000132471
株式会社セガ
東京都大田区羽田１丁目２番12号
(72)発明者　西岡　玄次
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100087170
弁理士　富田　和子

最終頁に続く

(54)【発明の名称】　コンテンツの利用制限解除方法および記憶媒体

(57)【要約】
【課題】ユーザに過度の負担をかけることなく、コンテンツの正規購入に先だってそのコンテンツを評価できるようにする。
【解決手段】一部の部分の利用を何らかの方法により制限したコンテンツを利用制限解除プログラムと共に記憶媒体４に格納してユーザに提供する。ユーザは、購入した記憶媒体４をユーザ端末１に装着し、コンテンツの利用可能な部分を実際に試すことができる。気に入った場合には、利用制限解除プログラムを起動させ、ネットワーク３を介して解除情報配信センタ２に前記コンテンツのタイトル名を含む解除依頼を送信し、当該コンテンツの解除情報を購入できる。そして、この利用制限解除プログラムによりコンテンツの利用制限を解除できる。

図1



1

【特許請求の範囲】

【請求項１】コンテンツを、一部を利用可能とし、その他の部分の利用を制限して、当該コンテンツの利用制限を解除するためのプログラムと共に記憶媒体に格納し、配布するステップと、

サーバが、ネットワークを介して、前記記憶媒体が装着された端末から解除依頼を受け付けると、当該記憶媒体に前記コンテンツと共に格納されている前記プログラムが当該コンテンツの利用制限を解除するのに使用する解除情報を、前記端末に送信するステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項２】記憶媒体が装着された端末にネットワークを介して接続されたサーバを用いて、当該記憶媒体に記憶されている、一部が利用可能であり、その他の部分の利用が制限されたコンテンツの利用制限を解除する、コンテンツの利用制限解除方法であって、

前記端末において、前記コンテンツの利用制限の解除依頼を前記サーバに送信する解除依頼ステップと、

前記サーバにおいて、前記端末より受信した解除依頼にしたがい、前記コンテンツの利用制限を解除するための解除情報を、当該コンテンツに固有の鍵を用いた暗号通信により前記端末と共有した鍵で暗号化し、前記端末に送信する解除情報送信ステップと、

前記端末において、前記サーバより受信した暗号文を、前記記憶媒体に記憶されている前記コンテンツに固有の鍵を用いた暗号通信により、前記サーバと共有した鍵で復号化し、その結果得られた解除情報を用いて、前記コンテンツの利用制限を解除する利用制限解除ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項３】請求項２記載のコンテンツの利用制限解除方法であって、

前記コンテンツは、前記その他の部分が暗号化されて、その利用が制限されたものであり、且つ、前記記憶媒体には、前記コンテンツと共に、共通鍵暗号体系に従った当該コンテンツに固有の鍵情報GKが記憶されており、

前記解除依頼ステップは、

乱数を用いて鍵K_iを生成し、当該鍵K_iと当該端末のユーザ情報ID_iとを含む情報を、前記記憶媒体から読み出した鍵情報GKを用いて暗号化し、その暗号結果である暗号文$C_{i,1}$と前記ユーザ情報ID_iとを、解除依頼として、前記サーバに送信するものであり、

前記解除情報送信ステップは、

予め用意してある前記コンテンツに固有の鍵情報GKを用いて、前記端末より受信した暗号文$C_{i,1}$を復号化し、その結果得られたユーザ情報ID_iと、前記暗号文$C_{i,1}$と共に送られてきたユーザ情報ID_iとを用いてユーザ認証を行うサーバ側ユーザ認証ステップと、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、前記コンテンツの暗号化部分を復号化するための復号鍵K（解除情報）と前記ユーザ情報ID_iとを含む情報を、前記暗号文$C_{i,1}$を復号化した結果得られた鍵K_iを用いて暗号化し、その暗号結果である暗号文$C_{i,2}$を、前記端末に送信する鍵送信ステップと、を有し、

前記利用制限解除ステップは、

前記解除依頼ステップで生成した暗号文$C_{i,1}$を前記記憶媒体から読み出した鍵情報GKを用いて復号化し、次いで、その結果得られた鍵K_iを用いて、前記サーバから受信した暗号文$C_{i,2}$を復号化し、その結果得られたユーザ情報ID_iを用いて、ユーザ認証を行う端末側ユーザ認証ステップと、

前記端末側ユーザ認証ステップでのユーザ認証が成立した場合に、前記暗号文$C_{i,2}$を復号化した結果得られた復号鍵Kを用いて、前記コンテンツの暗号化部分を復号化するコンテンツ復号化ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項４】請求項３記載のコンテンツの利用制限解除方法であって、

前記鍵送信ステップは、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、乱数Rを生成し、当該乱数Rと前記復号鍵Kと前記ユーザ情報ID_iとを、前記暗号文$C_{i,1}$を復号化した結果得られた鍵K_iを用いて暗号化し、その暗号結果である暗号文$C_{i,2}$を、前記端末に送信することを特徴とするコンテンツの利用制限解除方法。

【請求項５】請求項２記載のコンテンツの利用制限解除方法であって、

前記コンテンツは、前記その他の部分が暗号化されて、その利用が制限されたものであり、且つ、前記記憶媒体には、前記コンテンツと共に、共通鍵暗号体系に従った当該コンテンツに固有の鍵情報GK_1、GK_2が記憶されており、

前記解除依頼ステップは、

乱数を用いて鍵K_{i1}、K_{i2}を生成し、前記鍵K_{i2}を前記記憶媒体から読み出した鍵情報GK_2を用いて暗号化し、次いで、その暗号結果である暗号文$C_{0,1}$と前記鍵K_{i1}と当該端末のユーザ情報ID_iとを、前記記憶媒体から読み出した鍵情報GK_1を用いて暗号化し、その暗号結果である暗号文$C_{i,1}$と前記ユーザ情報ID_iとを、解除依頼として、前記サーバに送信するものであり、

前記解除情報送信ステップは、

予め用意してある前記コンテンツに固有の鍵情報GK_1を用いて、前記端末から受信した暗号文$C_{i,1}$を復号化し、その結果得られたユーザ情報ID_iと、前記暗号文$C_{i,1}$と共に送られてきたユーザ情報ID_iとを用いてユーザ認証を行うサーバ側ユーザ認証ステップと、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、予め用意してある前記コンテンツに固有の鍵情報GK_2を用いて、前記暗号文$C_{i,1}$を復号化した結果

2

得られた暗号文$C_{0,1}$を復号化し、その結果得られた鍵$K_{1,2}$を用いて前記コンテンツの暗号化部分を復号化するための復号鍵K（解除情報）を暗号化し、次いで、その暗号結果である暗号文$C_{0,2}$と前記ユーザ情報ID_iとを、前記暗号文$C_{1,1}$を復号化した結果得られた鍵$K_{i,1}$を用いて暗号化し、その結果得られた暗号文$C_{i,2}$を、前記端末に送信する鍵送信ステップと、を有し、

前記利用制限解除ステップは、

前記解除情報依頼送信ステップで生成した暗号文$C_{i,1}$を前記記憶媒体から読み出した鍵情報GK_1を用いて復号化し、次いで、その結果得られた鍵$K_{i,1}$を用いて前記サーバから受信した暗号文$C_{i,2}$を復号化し、その結果得られたユーザ情報ID_iを用いて、ユーザ認証を行う端末側ユーザ認証ステップと、

前記端末側ユーザ認証ステップでのユーザ認証が成立した場合に、前記暗号文$C_{i,1}$を復号化した結果得られた暗号文$C_{0,1}$を前記記憶媒体から読み出した鍵情報GK_2を用いて復号化し、その結果得られた鍵$K_{i,2}$を用いて、前記暗号文$C_{i,2}$を復号化した結果得られた暗号文$C_{0,2}$を復号化して、復号鍵Kを入手し、当該復号鍵Kを用いて前記コンテンツの暗号化部分を復号化するコンテンツ復号化ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項６】請求項２記載のコンテンツの利用制限解除方法であって、

前記記憶媒体には、前記コンテンツと共に、共通鍵暗号体系に従った当該コンテンツに固有の鍵情報GKと、当該コンテンツに固有の認証情報AKとが記憶されており、

前記解除依頼ステップは、

乱数を用いて鍵K_iを生成し、当該鍵K_iと当該端末のユーザ情報ID_iとを含む情報を、前記記憶媒体から読み出した鍵情報GKを用いて暗号化し、その暗号結果である暗号文$C_{i,1}$と前記ユーザ情報ID_iとを、解除依頼として、前記サーバに送信するものであり、

前記解除情報送信ステップは、

予め用意してある前記コンテンツに固有の鍵情報GKを用いて、前記端末より受信した暗号文$C_{i,1}$を復号化し、その結果得られたユーザ情報ID_iと、前記暗号文$C_{i,1}$と共に送られてきたユーザ情報ID_iとを用いてユーザ認証を行うサーバ側ユーザ認証ステップと、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、前記コンテンツの利用制限を解除するための認証情報AK（解除情報）と前記ユーザ情報ID_iとを含む情報を、前記暗号文$C_{i,1}$を復号化した結果得られた鍵K_iを用いて暗号化し、その暗号結果である暗号文$C_{i,2}$を、前記端末に送信する認証情報送信ステップと、を有し、

前記利用制限解除ステップは、

前記解除依頼ステップで生成した暗号文$C_{i,1}$を前記記憶媒体から読み出した鍵情報GKを用いて復号化し、次いで、その結果得られた鍵K_iを用いて、前記サーバから受信した暗号文$C_{i,2}$を復号化し、その結果得られたユーザ情報ID_iを用いて、ユーザ認証を行う端末側ユーザ認証ステップと、

前記端末側ユーザ認証ステップでのユーザ認証が成立した場合に、前記暗号文$C_{i,2}$を復号化した結果得られた認証情報AKと、前記記憶媒体に記憶されている認証情報AKとを比較して、両者が一致する場合に、前記コンテンツの利用が制限されている部分へのアクセスを許可するアクセス許可ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項７】請求項６記載のコンテンツの利用制限解除方法であって、

前記認証情報送信ステップは、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、乱数Rを生成し、当該乱数Rと前記認証情報AKと前記ユーザ情報ID_iとを、前記暗号文$C_{i,1}$を復号化した結果得られた鍵K_iを用いて暗号化し、その暗号結果である暗号文$C_{i,2}$を、前記端末に送信することを特徴とするコンテンツの利用制限解除方法。

【請求項８】請求項２記載のコンテンツの利用制限解除方法であって、

前記記憶媒体には、前記コンテンツと共に、共通鍵暗号体系に従った当該コンテンツに固有の鍵情報GK_1、GK_2と、当該コンテンツに固有の認証情報AKとが記憶されており、

前記解除依頼ステップは、

乱数を用いて鍵$K_{i,1}$、$K_{i,2}$を生成し、前記鍵$K_{i,2}$を前記記憶媒体から読み出した鍵情報GK_2を用いて暗号化し、次いで、その暗号結果である暗号文$C_{0,1}$と前記鍵$K_{i,2}$と当該端末のユーザ情報ID_iとを、前記記憶媒体から読み出した鍵情報GK_1を用いて暗号化し、その暗号結果である暗号文$C_{i,1}$と前記ユーザ情報ID_iとを、解除依頼として、前記サーバに送信するものであり、

前記解除情報送信ステップは、

予め用意してある前記コンテンツに固有の鍵情報GK_1を用いて、前記端末から受信した暗号文$C_{i,1}$を復号化し、その結果得られたユーザ情報ID_iと、前記暗号文$C_{i,1}$と共に送られてきたユーザ情報ID_iとを用いてユーザ認証を行うサーバ側ユーザ認証ステップと、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、予め用意してある前記コンテンツに固有の鍵情報GK_1を用いて、前記暗号文$C_{i,1}$を復号化した結果得られた暗号文$C_{0,1}$を復号化し、その結果得られた鍵$K_{1,2}$を用いて前記コンテンツの利用制限を解除するための認証情報AK（解除情報）を暗号化し、次いで、その暗号結果である暗号文$C_{0,2}$と前記ユーザ情報ID_iとを、前記暗号文$C_{i,1}$を復号化した結果得られた鍵$K_{i,1}$を用いて暗号化し、その結果得られた暗号文$C_{i,2}$を、前記端末に送信する認証情報送信ステップと、を有し、

5

前記利用制限解除ステップは、
前記解除依頼ステップで生成した暗号文$C_{1,1}$を前記記憶媒体から読み出した鍵情報GK_sを用いて復号化し、次いで、その結果得られた鍵K_{t1}を用いて前記サーバから受信した暗号文$C_{1,2}$を復号化し、その結果得られたユーザ情報ID_tを用いて、ユーザ認証を行う端末側ユーザ認証ステップと、
前記端末側ユーザ認証ステップでのユーザ認証が成立した場合に、前記暗号文$C_{1,1}$を復号化した結果得られた暗号文$C_{0,1}$を前記記憶媒体から読み出した鍵情報GK_sを用いて復号化し、その結果得られた鍵K_{t2}を用いて、前記暗号文$C_{1,2}$を復号化した結果得られた暗号文$C_{0,2}$を復号化して、認証情報AKを入手し、当該認証情報AKと前記記憶媒体に記憶されている認証情報AKとを比較して、両者が一致する場合に、前記コンテンツの利用が制限されている部分へのアクセスを許可するアクセス許可ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項９】記憶媒体が装着された端末にネットワークを介して接続されたサーバを用いて、当該記憶媒体に記憶されている、一部が利用可能であり、その他の部分の利用が制限されたコンテンツの利用制限を解除する、コンテンツの利用制限解除方法であって、
前記端末において、前記コンテンツの利用制限の解除依頼を前記サーバに送信する解除依頼ステップと、
前記サーバにおいて、前記端末から受信した解除依頼にしたがい、前記コンテンツの利用制限を解除するための解除情報を、当該コンテンツに固有の暗号鍵で暗号化し、前記端末に送信する解除情報送信ステップと、
前記端末において、前記サーバより受信した暗号文を、前記記憶媒体に記憶されている、前記コンテンツに固有の暗号鍵と対の復号鍵であって前記暗号鍵を推測不可能な復号鍵で、復号化し、その結果得られた解除情報を用いて、前記コンテンツの利用制限を解除する利用制限解除ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項１０】請求項９記載のコンテンツの利用制限解除方法であって、
前記コンテンツは、前記その他の部分が暗号化されて、その利用が制限されたものであり、且つ、前記記憶媒体には、前記コンテンツと共に、非対称鍵暗号体系に従った当該コンテンツに固有の鍵であって、当該鍵からは前記サーバが保持する当該鍵と対の暗号鍵K_sを推測不可能な復号鍵K_Tが記憶されており、
前記解除情報送信ステップは、
前記端末より受信した解除依頼に含まれるユーザ情報ID_tを用いて、ユーザ認証を行うサーバ側ユーザ認証ステップと、
前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、予め用意してある前記暗号鍵K_sを用いて、

6

前記端末より受信した解除依頼に含まれるユーザ情報ID_tと前記コンテンツの暗号化部分を復号化するための復号鍵K（解除情報）とを含む情報を暗号化し、その暗号結果である暗号文$C_{1,2}$を、前記端末に送信する鍵送信ステップと、を有し、
前記利用制限解除ステップは、
前記サーバから受信した暗号文$C_{1,2}$を前記記憶媒体から読み出した前記復号鍵K_Tを用いて復号化し、その結果得られたユーザ情報ID_tを用いて、ユーザ認証を行う端末側ユーザ認証ステップと、
前記端末側ユーザ認証ステップでのユーザ認証が成立した場合に、前記暗号文$C_{1,2}$を復号化した結果得られた復号鍵Kを用いて、前記コンテンツの暗号化部分を復号化するコンテンツ復号化ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項１１】請求項１０記載のコンテンツの利用制限解除方法であって、
前記鍵送信ステップは、
前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、乱数Rを生成し、当該乱数Rと前記復号鍵Kと前記ユーザ情報ID_tとを、予め用意してある前記暗号鍵K_sを用いて暗号化し、その暗号結果である暗号文$C_{1,2}$を、前記端末に送信することを特徴とするコンテンツの利用制限解除方法。

【請求項１２】請求項９記載のコンテンツの利用制限解除方法であって、
前記コンテンツは、前記その他の部分が暗号化されて、その利用が制限されたものであり、且つ、前記記憶媒体には、前記コンテンツと共に、非対称鍵暗号体系に従った当該コンテンツに固有の鍵であって、当該鍵からは、前記サーバが保持する当該鍵と対の暗号鍵K_{s1}、K_{s2}を、推測不可能な復号鍵K_{T1}、K_{T2}が記憶されており、
前記解除情報送信ステップは、
前記端末より受信した解除依頼に含まれるユーザ情報ID_tを用いて、ユーザ認証を行うサーバ側ユーザ認証ステップと、
前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、予め用意してある前記暗号鍵K_{s2}を用いて前記コンテンツの暗号化部分を復号化するための復号鍵K（解除情報）を暗号化し、次いで、その暗号結果である$C_{0,2}$と前記端末より受信した解除依頼に含まれるユーザ情報ID_tとを、予め用意してある前記暗号鍵K_{s1}を用いて暗号化し、その暗号結果である暗号文$C_{1,2}$を前記端末に送信する鍵送信ステップと、を有し、
前記利用制限解除ステップは、
前記サーバから受信した暗号文$C_{1,2}$を前記記憶媒体から読み出した前記復号鍵K_{T1}を用いて復号化し、その結果得られたユーザ情報ID_tを用いて、ユーザ認証を行う端末側ユーザ認証ステップと、
前記端末側認証ステップでのユーザ認証が成立した場合

に、前記暗号文$C_{i,2}$を復号化した結果得られた暗号文$C_{o,2}$を、前記記憶媒体から読み出した前記復号鍵K_{r2}を用いて復号化して、復号鍵Kを入手し、当該復号鍵Kを用いて、前記コンテンツの暗号化部分を復号化するコンテンツ復号化ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項１３】請求項９記載のコンテンツの利用制限解除方法であって、

前記記憶媒体には、前記コンテンツと共に、非対称鍵暗号体系に従った当該コンテンツに固有の鍵であって、当該鍵からは前記サーバが保持する当該鍵と対の暗号鍵K_sを推測不可能な復号鍵K_rと、当該コンテンツに固有の認証情報AKとが記憶されており、

前記解除情報送信ステップは、

前記端末より受信した解除依頼に含まれるユーザ情報ID$_u$を用いて、ユーザ認証を行うサーバ側ユーザ認証ステップと、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、予め用意してある前記暗号鍵K_sを用いて、前記端末より受信した解除依頼に含まれるユーザ情報ID$_u$と前記コンテンツの利用制限を解除するための認証情報AK（解除情報）とを含む情報を暗号化し、その暗号結果である暗号文$C_{i,2}$を、前記端末に送信する認証情報送信ステップと、を有し、

前記利用制限解除ステップは、

前記サーバから受信した暗号文$C_{i,2}$を前記記憶媒体から読み出した前記復号鍵K_rを用いて復号化し、その結果得られたユーザ情報ID$_u$を用いて、ユーザ認証を行う端末側ユーザ認証ステップと、

前記端末側ユーザ認証ステップでのユーザ認証が成立した場合に、前記暗号文$C_{i,2}$を復号化した結果得られた認証情報AKと、前記記憶媒体に記憶されている認証情報AKとを比較して、両者が一致する場合に、前記コンテンツの利用が制限されている部分へのアクセスを許可するアクセス許可ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項１４】請求項１３記載のコンテンツの利用制限解除方法であって、

前記認証情報送信ステップは、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、乱数Rを生成し、当該乱数Rと前記認証情報AKと前記ユーザ情報ID$_u$とを、予め用意してある前記暗号鍵K_sを用いて暗号化し、その暗号結果である暗号文$C_{i,2}$を、前記端末に送信することを特徴とするコンテンツの利用制限解除方法。

【請求項１５】請求項９記載のコンテンツの利用制限解除方法であって、

前記記憶媒体には、前記コンテンツと共に、非対称鍵暗号体系に従った当該コンテンツに固有の鍵であって、当該鍵からは、前記サーバが保持する当該鍵と対の暗号鍵

K_{s1}、K_{s2}を推測不可能な復号鍵K_{r1}、K_{r2}と、当該コンテンツに固有の認証情報AKとが記憶されており、

前記解除情報送信ステップは、

前記端末より受信した解除依頼に含まれるユーザ情報ID$_u$を用いて、ユーザ認証を行うサーバ側ユーザ認証ステップと、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、予め用意してある前記暗号鍵K_{s2}を用いて前記コンテンツの利用制限を解除するための認証情報AK（解除情報）を暗号化し、次いで、その暗号結果である$C_{o,2}$と前記端末より受信した解除依頼に含まれるユーザ情報ID$_u$とを、予め用意してある前記暗号鍵K_{s1}を用いて暗号化し、その暗号結果である暗号文$C_{i,2}$を前記端末に送信する認証情報送信ステップと、を有し、

前記利用制限解除ステップは、

前記サーバから受信した暗号文$C_{i,2}$を前記記憶媒体から読み出した前記復号鍵K_{r1}を用いて復号化し、その結果得られたユーザ情報ID$_u$を用いて、ユーザ認証を行う端末側ユーザ認証ステップと、

前記端末側ユーザ認証ステップでのユーザ認証が成立した場合に、前記暗号文$C_{i,2}$を復号化した結果得られた暗号文$C_{o,2}$を、前記記憶媒体から読み出した前記復号鍵K_{r2}を用いて復号化して、認証情報AKを入手し、当該認証情報AKと、前記記憶媒体に記憶されている認証情報AKとを比較して、両者が一致する場合に、前記コンテンツの利用が制限されている部分へのアクセスを許可するアクセス許可ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項１６】記憶媒体が装着された端末にネットワークを介して接続されたサーバを用いて、当該記憶媒体に記憶されている、一部が利用可能であり、その他の部分の利用が制限されたコンテンツの利用制限を解除する、コンテンツの利用制限解除方法であって、

前記端末において、任意の情報を含む前記コンテンツの利用制限の解除依頼を生成し、前記サーバに送信する解除依頼ステップと、

前記サーバにおいて、前記端末から受信した解除依頼に含まれる情報に対するデジタル署名を生成し、これを解除情報として、前記端末に送信する解除情報送信ステップと、

前記端末において、前記サーバより解除情報として送られてきたデジタル署名を検証し、その正当性が確認できた場合に、前記コンテンツの利用が制限されている部分へのアクセスを許可するアクセス許可ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項１７】一部が利用可能であり、その他の部分の利用が制限されたコンテンツと、

ネットワークを介して接続されたサーバにアクセスし、当該サーバから前記コンテンツの利用制限を解除するための解除情報を入手して、当該コンテンツの利用制限を

解除するプログラムと、を格納したことを特徴とする記憶媒体。

【請求項１８】コンテンツが記憶された記憶媒体であって、

前記コンテンツは、一部が利用可能であって、その他の部分の利用が制限されており、且つ、前記記憶媒体には、前記コンテンツの利用制限を解除する利用制限解除プログラムと、前記コンテンツに固有の鍵とが記憶されており、

前記利用制限解除プログラムは、前記記憶媒体が装着された端末に読み取られて実行されることで、

前記記憶媒体に記憶されている前記コンテンツに固有の鍵を用いた暗号通信により、当該端末にネットワークを介して接続されたサーバに、ユーザ情報ID_iと鍵K_iを含む解除依頼を送信する解除依頼手段と、

前記コンテンツの利用制限を解除するための解除情報とユーザ情報ID_iとを含む情報を前記鍵K_iで暗号化することで得られる暗号文$C_{i,2}$を、前記サーバから入手する解除情報入手手段と、

前記解除情報入手手段で入手した暗号文$C_{i,2}$を前記鍵K_iで復号化し、その結果得られたユーザ情報ID_iを用いてユーザ認証を行うユーザ認証手段と、

前記ユーザ認証手段でのユーザ認証が成立した場合に、前記暗号文$C_{i,2}$を復号化した結果得られた解除情報を用いて、前記コンテンツの利用制限を解除する利用制限解除手段とを、前記端末上に構築することを特徴とする記憶媒体。

【請求項１９】コンテンツが記憶された記憶媒体であって、

前記コンテンツは、一部が利用可能であって、その他の部分の利用が制限されており、且つ、前記記憶媒体には、前記コンテンツの利用制限を解除する利用制限解除プログラムと、前記コンテンツに固有の鍵であって当該鍵からは当該鍵と対の暗号鍵を推測不可能な鍵とが記憶されており、

前記利用制限解除プログラムは、前記記憶媒体が装着された端末に読み取られて実行されることで、

当該端末にネットワークを介して接続されたサーバに、ユーザ情報ID_iを含む解除依頼を送信する解除依頼手段と、

前記サーバから、前記コンテンツの利用制限を解除するための解除情報とユーザ情報ID_iとを含む情報を前記暗号鍵で暗号化することで得られる暗号文$C_{i,2}$を、入手する解除情報入手手段と、

前記解除情報入手手段で入手した暗号文$C_{i,2}$を、前記記憶媒体に記憶されている前記コンテンツに固有の鍵で復号化し、その結果得られたユーザ情報ID_iを用いてユーザ認証を行うユーザ認証手段と、

前記ユーザ認証手段でのユーザ認証が成立した場合に、前記暗号文$C_{i,2}$を復号化した結果得られた解除情報を用いて、前記コンテンツの利用制限を解除する利用制限解除手段とを、前記端末上に構築することを特徴とする記憶媒体。

【請求項２０】請求項１８または１９記載の記憶媒体であって、

当該記憶媒体に記憶されるコンテンツに固有の鍵は、定期的に、もしくは、当該コンテンツが更新される都度、更新されることを特徴とする記憶媒体。

【請求項２１】請求項１８、１９または２１記載の記憶媒体であって、

前記ユーザ認証手段は、前記端末が、前記記録媒体に記録されている前記コンテンツの利用が制限されている部分にアクセスする都度、実行され、

前記利用制御解除手段は、前記ユーザ認証手段でのユーザ認証が成立する都度、前記端末がアクセスしようとしている部分についての利用制限を解除することを特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、アプリケーションプログラムやマルチメディアデータ等のコンテンツの利用を制限する技術に関し、特に、ユーザに過度の負担をかけることなく、コンテンツの正規購入に先だってそのコンテンツを評価できるようにするのに好適な技術に関する。

【０００２】

【従来の技術】近年、アプリケーションプログラムやマルチメディアデータ等のコンテンツが、ＣＤ-ＲＯＭやＤＶＤ-ＲＯＭ等の記憶媒体に格納されて販売されている。この種のコンテンツは電子データであるため、ユーザは、コンテンツの評価などを行う雑誌で調べてみても、実際に使用してみないと、それが有益であるか否かを判断できないことが多い。このため、従来、この種の雑誌には、コンテンツの一部のみ利用可能にしたものが格納された記憶媒体、いわゆるお試し版が添付されたりしている。

【０００３】

【発明が解決しようとする課題】しかしながら、上記の従来によれば、ユーザは、コンテンツの正規購入に先だってそのコンテンツを評価したい場合、本屋等でこの種の雑誌を購入し、それに添付されている前記コンテンツのお試し版を使用してみなければならない。そして、気に入った場合には、このお試し版とは別途に、ソフト販売店等で、前記コンテンツが格納された記憶媒体を購入しなければならない。つまり、上記の従来によれば、ユーザに、正規コンテンツの購入以外に、雑誌等購入の手間や金銭的な負担をかけるている。

【０００４】本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、ユーザに過度の負担をかけることなく、コンテンツの正規購入に先だってそのコンテ

ンツを評価できるようにすることにある。

【０００５】

【課題を解決するための手段】上記課題を解決するために、本発明では、アプリケーションプログラムやマルチメディアデータ等のコンテンツを、一部利用可能とし、その他の部分の利用を制限して、ＣＤ-ＲＯＭやＤＶＤ-ＲＯＭ等の記憶媒体に格納し、ユーザに提供する。前記記憶媒体が装着されたネットワーク接続機能を有する端末は、ユーザの指示にしたがい、ネットワークを介してサーバにアクセスして、当該サーバから前記コンテンツの利用制限を解除するための解除情報を入手する。そして、当該解除情報を用いて前記コンテンツの利用制限を解除する。

【０００６】本発明によれば、ユーザは、前記端末に前記記憶媒体を装着し、当該コンテンツの利用可能な部分を実際に使用してみて、当該コンテンツを評価することができる。ここで、ＣＤ-ＲＯＭやＤＶＤ-ＲＯＭ等の記憶媒体自体の製造コストは、コンテンツ自体の対価に比べて安価である。したがって、そのままでは（解除情報を入手しなければ）一部しか利用できないコンテンツが格納された前記記憶媒体を、例えば、記録媒体自体の製造コストと流通コストを考慮した、比較的安価な値段でユーザに提供することがきる。

【０００７】また、ユーザは、前記コンテンツの利用可能な部分を実際に使用してみて、当該コンテンツを評価した結果、当該コンテンツを気に入った場合、当該コンテンツを格納した前記記憶媒体が装着された前記端末を用い、ネットワークを介してサーバにアクセスして、当該サーバから前記コンテンツの利用制限を解除するための解除情報を入手することにより、前記コンテンツの利用制限を解除することができる。つまり、ユーザは、全ての部分が利用可能に構成された正規のコンテンツが記憶された記憶媒体を別途購入しなくても済む。ここで、解除情報の対価は、例えば、前記コンテンツを格納する記憶媒体自体の製造コストと流通コストを除いた、当該コンテンツ自体に対する対価に設定することができる。

【０００８】したがって、本発明によれば、ユーザに過度の負担をかけることなく、コンテンツの正規購入に先だってそのコンテンツを評価することが可能となる。つまり、上記の従来で説明したような、正規コンテンツの購入以外の雑誌等購入の手間や金銭的な負担を低減することができる。

【０００９】なお、本発明において、前記記憶媒体が装着された前記端末が、ネットワークを介してサーバにアクセスして、当該サーバから前記コンテンツの利用制限を解除するための解除情報を入手し、当該コンテンツの利用制限を解除するためのプログラムは、前記コンテンツと共に前記記憶媒体に格納しておくようにするとよい。このようにすれば、前記端末自体に、前記サーバから解除情報を入手して前記コンテンツの利用制限を解除するための専用のハードウエア構成を設ける必要がなくなる。つまり、ネットワーク接続機能を有するゲーム機やパーソナルコンピュータなどの汎用の電子計算機を前記端末に利用することが可能となる。

【００１０】より具体的に説明すると、本発明の第１の態様では、記憶媒体が装着された端末にネットワークを介して接続されたサーバを用いて、当該記憶媒体に記憶されている、一部が利用可能であり、その他の部分の利用が制限されたコンテンツの利用制限を解除する、コンテンツの利用制限解除方法であって、前記端末において、前記コンテンツの利用制限の解除依頼を前記サーバに送信する解除依頼ステップと、前記サーバにおいて、前記端末より受信した解除依頼にしたがい、前記コンテンツの利用制限を解除するための解除情報を、当該コンテンツに固有の鍵を用いた暗号通信により前記端末と共有した鍵で暗号化し、前記端末に送信する解除情報送信ステップと、前記端末において、前記サーバより受信した暗号文を、前記記憶媒体に記憶されている前記コンテンツに固有の鍵を用いた暗号通信により、前記サーバと共有した鍵で復号化し、その結果得られた解除情報を用いて、前記コンテンツの利用制限を解除する利用制限解除ステップと、を有する。

【００１１】本態様によれば、前記記憶媒体に前記コンテンツと共に記憶されている当該コンテンツに固有の鍵を用いて解除情報を、前記サーバから前記端末へ送信するようにしている。したがって、同じコンテンツであれば、当該コンテンツと共に前記記録媒体に記憶する鍵も同じものになる。つまり、記憶媒体毎に固有の情報を当該記憶媒体に記憶させる必要がないので、前記記憶媒体を例えばプレス等により大量生産するのに好適である。

【００１２】また、本発明の第２の態様では、記憶媒体が装着された端末にネットワークを介して接続されたサーバを用いて、当該記憶媒体に記憶されている、一部が利用可能であり、その他の部分の利用が制限されたコンテンツの利用制限を解除する、コンテンツの利用制限解除方法であって、前記端末において、前記コンテンツの利用制限の解除依頼を前記サーバに送信する解除依頼ステップと、前記サーバにおいて、前記端末から受信した解除依頼にしたがい、前記コンテンツの利用制限を解除するための解除情報を、当該コンテンツに固有の暗号鍵で暗号化し、前記端末に送信する解除情報送信ステップと、前記端末において、前記サーバより受信した暗号文を、前記記憶媒体に記憶されている、前記コンテンツに固有の暗号鍵と対の復号鍵であって前記暗号鍵を推測不可能な復号鍵で、復号化し、その結果得られた解除情報を用いて、前記コンテンツの利用制限を解除する利用制限解除ステップと、を有する。

【００１３】本態様においても、上記の第１の態様と同様、同じコンテンツであれば、当該コンテンツと共に前記記録媒体に記憶する鍵も同じものになるので、つま

り、記憶媒体毎に固有の情報を当該記憶媒体に記憶させる必要がないので、前記記憶媒体を例えばプレス等により大量生産するのに好適である。

【００１４】加えて、本態様によれば、前記記憶媒体に記憶される鍵を、当該鍵からは前記サーバが保持する対の暗号鍵を推測不可能な復号鍵としている。したがって、例えば不正な第３者が前記記憶媒体の内容を解析して前記復号鍵を入手したとしても、当該復号鍵からこれと対の暗号鍵を求めることができない以上、当該第３者が、前記復号鍵で復号可能な解除情報を含む暗号文を生成することはできない。つまり、当該第３者が前記サーバの運営者になりすますのを防ぐことができる。

【００１５】

【発明の実施の形態】まず、以下に説明する本発明の各実施形態が適用されるコンテンツ利用制限解除システムの概略について、図１を用いて説明する。

【００１６】図１は、本発明の各実施形態が適用されるコンテンツ利用制限解除システムの概略構成図である。

【００１７】図示するように、このコンテンツ利用制限解除システムは、ユーザ端末１と、ソフトメーカ５もしくはソフトメーカ５からの依頼を受けた者が運営する解除情報配信センタ２とが、ネットワーク３を介して、互いに接続されて構成されている。なお、ここでは、ユーザ端末１および解除情報配信センタ２をそれぞれ１つ示しているが、当然のことながら、複数であっても構わない。

【００１８】ソフトメーカ５は、一部を利用可能とし、その他の部分の利用を何らかの方法により制限した、アプリケーションプログラム（例えばゲーム）やマルチメディアデータ（例えばビデオ）等のコンテンツを、その利用制限を解除するための利用制限解除プログラムと共に、ＣＤ-ＲＯＭやＤＶＤ-ＲＯＭ等の記憶媒体４に格納して、例えばソフト販売店６等経由でユーザ７に提供する。また、コンテンツの利用制限を解除するための解除情報とそのコンテンツのタイトル名とを、暗号通信や郵送等のセキュリティが確保される方法により、解除情報配信センタ２に知らせる。解除情報配信センタ２は、ソフトメーカ５から通知されたコンテンツのタイトル名とその解除情報とを対応付けて記憶装置等に記憶し管理する。

【００１９】なお、ＣＤ-ＲＯＭやＤＶＤ-ＲＯＭ等の記憶媒体４自体の製造コストは、コンテンツの対価に比べて安価であり、また、記憶媒体４に格納されているコンテンツは、そのままでは（解除情報を入手しなければ）一部しか利用できないものであるので、記録媒体４の値段を、例えば、記録媒体４自体の製造コストと当該記録媒体４の流通コストとを考慮した、比較的安価な値段に設定し、ユーザ７に提供することができる。

【００２０】ユーザ７は、ソフト販売店６等で購入した記憶媒体４を、ユーザ端末１に装着し、当該記憶媒体４に格納されているコンテンツの利用可能な部分を実際に試してみて、当該コンテンツを評価することができる。気に入った場合には、ユーザ端末１に、当該記録媒体４中に格納されている利用制限解除プログラムを起動させることにより、ネットワーク３を介して解除情報配信センタ２に前記コンテンツのタイトル名を含む解除依頼を送信し、解除情報配信センタ２から当該コンテンツの解除情報を購入することができる。そして、この利用制限解除プログラムにより、購入した解除情報を使って対応するコンテンツの利用制限を解除することで、コンテンツの全ての部分が利用可能になる。

【００２１】なお、解除情報の値段は、例えば記憶媒体４自体の製造コストと記録媒体４の流通コストを除いたコンテンツ自体の値段に設定することができる。したがって、従来の技術で説明したような、正規コンテンツの購入以外の雑誌等購入の手間や金銭的な負担をユーザにかけなくて済む。

【００２２】また、解除情報配信センタ２に解除依頼を送信して解除情報を購入し、コンテンツの利用制限を解除するための利用制限解除プログラムは、当該コンテンツと共に記録媒体４に格納されているので、ユーザ端末１にそのための専用ハードウエア構成を設ける必要がなくなる。つまり、ネットワーク接続機能を有するテレビゲーム機やパーソナルコンピュータなどの汎用の電子計算機をユーザ端末１として利用することが可能となる。

【００２３】以下に、上述したコンテンツ利用制限解除システムの、より具体的な実施形態について説明する。

【００２４】先ず、本発明の第１実施形態について説明する。

【００２５】本実施形態では、記憶媒体４に格納するコンテンツの利用制限を暗号化により実現している。そして、当該コンテンツの暗号化部分を復号するための復号鍵（解除情報）を、共通鍵暗号体系に従った当該コンテンツに固有の鍵情報を用いた、暗号通信により、解除情報配信センタ２からユーザ端末１へ送信するようにしている。

【００２６】まず、記憶媒体４のデータ構成について説明する。

【００２７】図２は、本実施形態で用いられる記憶媒体４のデータ構成図である。

【００２８】図示するように、記憶媒体４には、コンテンツ４１と利用制限解除プログラム４２が格納される。コンテンツ４１は、ゲーム等のアプリケーションプログラム４１１と、そのアプリケーションプログラム４１１が使用するアプリケーションデータ４１２とを有する。アプリケーションデータ４１２は、一部を残してその他の部分が暗号化されている。また、利用制限解除プログラム４２は、鍵生成プログラム４２１と、鍵情報入手プログラム４２２と、コンテンツ復号化プログラム４２３と、共通鍵暗号体系に従った、コンテンツ４１に固有の

鍵情報GK４２４と、を有する。なお、ここでは、いわゆるバーションの相違も異なるコンテンツとみなしている。

【００２９】次に、ユーザ端末１について説明する。

【００３０】図３に、ユーザ端末１のハードウエア構成の一例を示す。

【００３１】なお、上述したように、ユーザ端末１には、ネットワーク接続機能を有するテレビゲーム機やパーソナルコンピュータなどの汎用の電子計算機を利用することができる。ここでは、ユーザ端末１がテレビゲーム機である場合の一例を示している。

【００３２】図３において、ＣＰＵ１１は、本ユーザ端末１の各部を統括的に制御する。メモリ１２は、ＣＰＵ１１のワークエリアとして機能する。フラッシュメモリ１３には、オペレーティングシステム（ＯＳ）プログラムと、本ユーザ端末１の識別情報ID_tとが格納されている。また、本ユーザ端末１のユーザより受け付けたユーザの個人情報ID_uが格納される。

【００３３】通信装置１４は、ネットワーク３を介して、解除情報配信センタ２にアクセスし、解除情報配信センタ２から解除情報（コンテンツ４１を復号するための鍵）入手するのに用いられる。

【００３４】入力装置１６は、各種操作ボタンを備えたコントローラで構成され、ユーザからのコンテンツ４１の利用指示や解除情報の入手指示等を受け付ける。

【００３５】読取装置１９には、記憶媒体４が装着され、当該記憶媒体４から利用制限解除プログラム４２やコンテンツ４１を読み出す。

【００３６】オーディオ再生装置１６は、読取装置１９より読み出されたコンテンツ４１を再生してオーディオ信号を生成する。また、ＣＰＵ１２からの指示にしたがい、図示していないサウンドバッファに格納されている波形データ等を利用してオーディオ信号を生成する。

【００３７】ビデオ再生装置１７は、読取装置１９より読み出されたコンテンツ４１を再生してビデオ信号を生成する。また、ＣＰＵ１２からの描画指示にしたがい、図示していないテクスチャバッファに格納されているテクスチャデータ等を利用して描画を行い、そのビデオ信号を生成する。

【００３８】カード接続装置１８は、メモリカード２０を接続し、当該メモリカード２０に解除情報を格納したり、当該メモリカード３０に格納された解除情報を読み出したりする。

【００３９】インターフェース２１は、ＣＰＵ１１やメモリ１２やフラッシュメモリ１３と本ユーザ端末１を構成する他装置との間のデータ送受を司る。

【００４０】図４に、ユーザ端末１上に構築されるソフトウエア構成を示す。

【００４１】この図に示す各構成要素は、フラッシュメモリ１３に格納されているＯＳプログラムが稼動している状態で、読取装置１９により記憶媒体４から読み出され、メモリ１２上にロードされた、利用制限解除プログラム４２およびアプリケーションプログラム４１１を、ＣＰＵ１１が実行することにより、プロセスとして具現化される。

【００４２】鍵生成部１１１は、鍵生成プログラム４２１により実現される。乱数を生成して鍵K_tを生成する。

【００４３】解除情報入手部１１２は、解除情報入手プログラム４２１により実現される。記憶媒体４に格納されている鍵情報GKを用いた共通鍵暗号による暗号通信により、解除情報配信センタ２よりコンテンツ４１復号化のための鍵K（解除情報）を入手する。

【００４４】コンテンツ復号化部１１３は、コンテンツ復号化プログラム４２３により実現される。解除情報入手部１１２で入手した鍵Kを用いて、記憶媒体４に格納されているアプリケーションデータ４１２の暗号化部分を復号する。

【００４５】アプリ処理部１１５は、アプリケーションプログラム４１１により実現され、アプリケーションプログラム４１１の内容に応じた処理（たとえば、アプリケーションプログラム４１１がゲームプログラムならばゲームの実行）を行う。

【００４６】主制御部１１４は、ＯＳにより実現され、図３に示す本ユーザ端末１の各ハードウエア構成要素を統括的に制御する。また、鍵生成部１１１や解除情報入手部１１２やコンテンツ復号化部１１３やアプリ処理部１１５に指示を出す。

【００４７】次に、解除情報配信センタ２について説明する。

【００４８】解除情報配信センタ２のハードウエア構成は、例えば、図３において、オーディオ再生装置１６やビデオ再生装置１７やカード接続装置１８やフラッシュメモリ１９が省略され、その代わりにハードディスク等の記憶装置が設けられた、一般的な構成を有する電子計算機を利用することができる。

【００４９】図５に、解除情報配信センタ２上に構築されるソフトウエア構成を示す。

【００５０】解除情報送信部２１１は、後述する管理テーブル２１２に格納されている鍵情報GKを用いた共通鍵暗号による暗号通信により、コンテンツ復号化のための鍵K（解除情報）を送信する。

【００５１】管理テーブル２１２には、ソフトメーカ５より通知されたコンテンツ４１のタイトル名２１２ａと、そのバージョン名２１２ｂと、タイトル名２１２ａおよびバージョン名２１２ｂにより特定されるコンテンツ４１にユニークに割り当てられた、共通鍵暗号体系に従った鍵情報GK２１２ｃと、当該コンテンツ４１の暗号化部分を復号するための鍵K２１２ｄが、互いに対応付けられて、リスト形式で登録・管理されている。

【００５２】課金処理部２１３は、解除情報送信部２１

１にてコンテンツ４１復号化のための鍵K２１２ｄを送信したユーザ端末１のユーザに対する課金処理を行う。

【００５３】なお、上記の解除情報送信部２１１や課金処理部２１３は、予めハードディスク等の記憶装置に格納されているＯＳが稼動している状態で、所定のプログラムが前記記憶装置あるいは読取装置を介して記憶媒体から読み出されてメモリ上にロードされ、それをＣＰＵが実行することにより、プロセスとして具現化される。また、管理テーブル２１２には、前記記憶装置等が利用される。

【００５４】次に、本実施形態の動作について説明する。

【００５５】本実施形態の動作は、ユーザ端末１において、鍵情報配信センタ２に送信する解除依頼中に含める情報を生成する解除依頼生成処理、ユーザ端末１が、前記解除依頼生成処理で生成した情報を含んだ解除依頼を鍵情報配信センタ２に送信して、鍵情報配信センタ２から鍵K（解除情報）を入手する解除情報入手処理、および、入手した鍵Kを用いてコンテンツ４１の暗号化部分を復号化するコンテンツ復号化処理の３つに分けられる。

【００５６】まず、解除依頼生成処理について説明する。

【００５７】図６は、本実施形態の解除依頼生成処理を説明するための図である。

【００５８】ユーザ端末１において、主制御部１１４は、入力装置１５を介してユーザより解除依頼生成の指示を受け付けると、鍵生成部１１１に指示を出す。これを受けて、鍵生成部１１１は、乱数により鍵K_iを生成し、これを解除情報入手部１１２に渡す（ステップＳ１００１）。

【００５９】次に、解除情報入手部１１２は、主制御部１１４を介して、フラッシュメモリ１３からユーザの個人情報ID_iを読み出すと共に、記憶媒体４から鍵情報GK４２４を読み出す。そして、共通鍵暗号体系にしたがい、鍵生成部１１１から受け取った鍵K_iとユーザの個人情報ID_iとを繋げたデータ（$K_i \| ID_i$）を、鍵情報GK４２４を用いて暗号化し、暗号文$C_{i,1}$（$=E_{GK}(K_i \| ID_i)$）を生成する（ステップＳ１００２）。

【００６０】次いで、解除情報入手部１１２は、生成した暗号文$C_{i,1}$を、主制御部１１４を介してメモリカード２０に格納し（ステップＳ１００３）、その後、メモリ１２上のワークエリアから鍵K_iを除去して処理を終了する（ステップＳ１００４）。

【００６１】次に、解除情報入手処理について説明する。

【００６２】図７および図８は、本実施形態の解除情報入手処理を説明するための図であり、図７はユーザ端末１側での処理を、そして、図８は鍵情報配信センタ２側での処理を示している。

【００６３】まず、ユーザ端末１において（図７参照）、主制御部１１４は、入力装置１５を介してユーザより解除情報入手の指示を受け付けると、解除情報入手部１１２に指示を出す。これを受けて、解除情報入手部１１２は、主制御部１１４を介して、フラッシュメモリ１３からユーザの個人情報ID_iを読み出すと共に、記憶媒体４からコンテンツ４１のタイトルおよびバージョン名を読み出す。また、メモリカード２０から、解除依頼生成処理で作成した暗号文$C_{i,1}$（$=E_{GK}(K_i \| ID_i)$）を読み出す。そして、ユーザの個人情報ID_i、コンテンツのタイトルおよびバージョン名、および、暗号文$C_{i,1}$を含んだ解除依頼を作成し（ステップＳ１１０１）、解除情報配信センタ２に送信する（ステップＳ１１０２）。

【００６４】解除情報配信センタ２において（図８参照）、解除情報送信部２１１は、ユーザ端末１より解除依頼を受信すると（ステップＳ１２０１）、当該解除依頼に含まれているコンテンツのタイトルおよびバージョン名に対応する鍵情報GK２１２ｃ（これは当該コンテンツを格納する記憶媒体４の利用制限解除プログラム４２に格納されている鍵情報GK４２４と一致する）を読出し、この鍵情報GKを用いて、前記解除依頼に含まれている暗号文$C_{i,1}$を復号化する。これにより、鍵K_iとユーザの個人情報ID_iを得る（ステップＳ１２０２）。

【００６５】それから、課金処理部２１３は、解除依頼を送信したユーザ端末１のユーザの認証を行う（ステップＳ１２０３）。例えば、受信した解除依頼に含まれているユーザの個人情報ID_iが正規のユーザとして記憶装置等に登録されているか否かを調べ、登録されているならば、当該個人情報ID_iとステップＳ１２０２で暗号文$C_{i,1}$を復号化した結果得られたユーザの個人情報ID_iとを比較する。そして、両者が一致する場合は、ユーザ認証が成立したものとする。

【００６６】ユーザ認証が成立しなかった場合（ステップＳ１２０４でＮｏ）は、その旨を解除情報送信部２１１に知らせて、前記解除依頼を送信したユーザ端末１にエラー通知を送信する（ステップＳ１２０５）。

【００６７】一方、ユーザ認証が成立した場合（ステップＳ１２０４でＹｅｓ）は、そのユーザの個人情報ID_iにより特定されるユーザに対して課金処理を行い（ステップＳ１２０６）、その旨を解除情報送信部２１１に知らせる。解除情報送信部２１１は、受信した解除依頼に含まれているコンテンツのタイトルおよびバージョン名に対応する鍵K２１２ｄ（これが当該タイトルおよびバージョン名により特定されるコンテンツ４１のアプリケーションデータ４１２の暗号化部分を復号化するための鍵（解除情報）である）を読出し、この鍵Kと前記ユーザの個人情報ID_iとを繋げたデータ（$K \| ID_i$）を、ステップＳ１２０２で暗号文$C_{i,1}$を復号化した結果得られた鍵K_iを用いて暗号化し、暗号文$C_{i,2}$（$=E_{K_i}(K \| ID_i)$）を生成して（ステップＳ１２０７）、前記解除依頼を送信

したユーザ端末１に送信する（ステップＳ１２０８）。

【００６８】ユーザ端末１において（図７参照）、解除情報入手部１１２は、解除情報配信センタ２より情報を受信すると（ステップＳ１１０３）、それがエラー通知ならば（ステップＳ１１０４でＮｏ）、その旨を本ユーザ端末１に接続されているテレビ等に出力するなど所定のエラー処理を行う（ステップＳ１１０５）。一方、暗号文$C_{i,2}$ならば（ステップＳ１１０４でＹｅｓ）、記憶媒体４から鍵情報GK４２４を読み出すと共に、メモリカード２０から、解除依頼生成処理で作成した暗号文$C_{i,1}$（$=E_{G_K}(K_i \| ID_i)$）を読み出す。そして、この鍵情報GKを用いて暗号文$C_{i,1}$を復号化し、鍵K_iとユーザの個人情報ID_iを得る（ステップＳ１１０６）。次に、この鍵K_iを用いて、鍵情報配信センタ２より受信した暗号文$C_{i,2}$（$=E_{K_i}(K \| ID_i)$）を復号化し、コンテンツ４１復号化のための鍵Kとユーザの個人情報ID_iを得る（ステップＳ１１０７）。

【００６９】それから、解除情報入手部１１２は、ステップＳ１１０６で暗号文$C_{i,1}$を復号化することで得たユーザの個人情報ID_iと、ステップＳ１１０７で暗号文$C_{i,2}$を復号化することで得たユーザの個人情報ID_iとを比較し、両者の一致を調べることで、ユーザ認証を行う（ステップＳ１１０８）。

【００７０】ユーザ認証が成立しなかった場合（ステップＳ１１０９でＮｏ）は、その旨を本ユーザ端末１に接続されているテレビ等に出力するなど所定のエラー処理を行い、それから、メモリ１２上のワークエリアから鍵K_iを除去して処理を終了する（ステップＳ１１０５）。

【００７１】一方、ユーザ認証が成立した場合（ステップＳ１１０９でＹｅｓ）は、鍵情報配信センタ２より受信した暗号文$C_{i,2}$を、主制御部１１４を介してメモリカード２０に、当該メモリカード２０に既に格納されている暗号文$C_{i,1}$と共に格納し（ステップＳ１１１０）、それから、メモリ１２上のワークエリアから鍵K_iを除去して処理を終了する（ステップＳ１１１１）。

【００７２】次に、コンテンツ復号化処理について説明する。

【００７３】図９は、本実施形態のコンテンツ復号化処理を説明するための図である。

【００７４】ユーザ端末１において、コンテンツ復号化部１１３は、アプリ処理部１１５によるアプリケーションデータ４１２の暗号化部分へのアクセスを監視する（ステップＳ１３０１）。そして、アプリ処理部１１５がアプリケーションデータ４１２の暗号化部分へアクセスし、主制御部１１４が暗号化データを読み出した場合には、これをフェッチする。

【００７５】次に、コンテンツ復号化部１１３は、主制御部１１４を介して、メモリカード２０から暗号文$C_{i,1}$を読み出すと共に、記憶媒体４から鍵情報GK４２４を読出す。そして、この鍵情報GKを用いて暗号文$C_{i,1}$を復号化することにより、鍵K_iとユーザの個人情報ID_iを得る（ステップＳ１３０２）。

【００７６】それから、コンテンツ復号化部１１３は、主制御部１１４を介してフラッシュメモリ１３からユーザの個人情報ID_iを読み出して、これとステップＳ１３０２で暗号文$C_{i,1}$を復号化することで得たユーザの個人情報ID_iとを比較し、両者の一致を調べることで、ユーザ認証を行う（ステップＳ１３０３）。

【００７７】ユーザ認証が成立しなかった場合（ステップＳ１３０４でＮｏ）は、ステップＳ１３０１でフェッチした暗号化データをアプリ処理部１１５に渡し、その後、メモリ１２上のワークエリアから鍵K、K_iを除去して、ステップＳ１３０１に戻る。

【００７８】一方、ユーザ認証が成立した場合（ステップＳ１３０４でＹｅｓ）は、主制御部１１４を介してメモリカード２０から暗号文$C_{i,2}$を読み出し、これをステップＳ１３０２で得た鍵K_iを用いて復号化し、コンテンツ復号化のための鍵Kとユーザの個人情報ID_iを得る（ステップＳ１３０５）。

【００７９】それから、コンテンツ復号化部１１３は、ステップＳ１３０２で暗号文$C_{i,1}$を復号化することで得たユーザの個人情報ID_iと、ステップＳ１３０５で暗号文$C_{i,2}$を復号化することで得たユーザの個人情報ID_iとを比較し、両者の一致を調べることで、ユーザ認証を行う（ステップＳ１３０６）。

【００８０】ユーザ認証が成立しなかった場合（ステップＳ１３０７でＮｏ）は、ステップＳ１３０１でフェッチした暗号化データをアプリ処理部１１５に渡し、その後、メモリ１２上のワークエリアから鍵K、K_iを除去して、ステップＳ１３０１に戻る。

【００８１】一方、ユーザ認証が成立した場合（ステップＳ１３０７でＹｅｓ）は、ステップS１３０１でフェッチした暗号化データを、ステップＳ１３０５で得た鍵Kを用いて復号化する（ステップＳ１３０８）。そして、復号化したデータをアプリ処理部１１５に渡した後、メモリ１２上のワークエリアから鍵K、K_iを除去して、ステップＳ１３０１に戻る。

【００８２】以上、本発明の第１実施形態について説明した。

【００８３】本実施形態によれば、記憶媒体４にコンテンツ４１と共に記憶されている当該コンテンツ４１に固有の鍵情報GKと、ユーザ端末１のユーザの個人情報ID_iとを用いて、当該ユーザ端末１のユーザのみが利用できる（ユーザ認証をパスできる）解除情報(鍵K)を、解除情報配信センタ２からユーザ端末１へ送信するようにしている。したがって、タイトル名およびバージョンが同じコンテンツ４１であれば、当該コンテンツ４１と共に記録媒体４に記憶する鍵情報GKも同じものになる。つまり、記憶媒体４毎に固有の情報を当該記憶媒体４に記憶させる必要がないので、ＣＤ-ＲＯＭやＤＶＤ-ＲＯＭ等

の記憶媒体４を、例えばプレス等により大量生産するのに好適である。

【００８４】また、ユーザ端末１において、コンテンツ復号化部１１３は、アプリ処理部１１５によるアプリケーションデータ４１２の暗号化部分へのアクセスを監視し、前記アクセスがあった場合に、主制御部１１４を介して記憶媒体４から読み出された暗号化データを復号化するようにしている。つまり、アプリケーションデータ４１２の暗号化部分の復号を、アプリ処理部１１５での処理中に、アプリ処理部１１５が要求するアプリケーションデータ４１２が暗号化されているか否かに応じてダイナミックに行うことができる。

【００８５】なお、上記の第１実施形態では、ユーザ端末１が解除情報配信センタ２に送信する解除情報に含まれる暗号文$C_{i,1}$を、鍵生成部１１１から受け取った鍵K_iとユーザの個人情報ID_iとを繋げたデータ（$K_i \| ID_i$）を鍵情報GK４２４で暗号化することで作成している。しかしながら、鍵K_iとユーザの個人情報ID_iにその他のデータを繋げたデータを鍵情報GK４２４で暗号化することで、暗号文$C_{i,1}$を作成するようにしてもよい。

【００８６】例えば、ユーザ端末１のフラッシュメモリ１３等にユーザ端末１の識別情報ID_tが格納されている場合は、鍵K_iとユーザの個人情報ID_iとユーザ端末１の識別情報ID_tとを繋げたデータ（$K_i \| ID_i \| ID_t$）を、鍵情報GK４２４を用いて暗号化して、暗号文$C_{i,1}$を作成するようにしてもよい。そして、この識別情報ID_tを解除依頼に加えて解除情報配信センタ２に送信し、当該解除情報配信センタ２において、ユーザの個人情報ID_iに加えてユーザ端末１の識別情報ID_tをも利用して、ユーザ認証を行うようにしてもよい。

【００８７】あるいは、鍵生成部１１１に鍵K_iと共に乱数Rを生成させ、鍵K_iとユーザの個人情報ID_iと乱数Rを繋げたデータ（$K_i \| ID_i \| R$）を、鍵情報GK４２４を用いて暗号化して、暗号文$C_{i,1}$を作成するようにしてもよい。このようにすれば、暗号文$C_{i,1}$から鍵K_iが不正に解読される可能性をより低くできる。

【００８８】また、解除情報配信センタ２からユーザ端末１へ送信される暗号文$C_{i,2}$についても同様に、例えば解除情報送信部２１１に乱数Rを生成させ、鍵Kとユーザの個人情報ID_iと乱数Rを繋げたデータ（$K \| ID_i \| R$）を、鍵K_iを用いて暗号化することで、作成するようにしてもよい。このようにすれば、暗号文$C_{i,2}$から鍵Kが不正に解読される可能性をより低くできる。

【００８９】また、上記の第１実施形態では、コンテンツのタイトルのみならずバージョンが異なる場合でも、鍵情報GKが異なるようにしているが、これに限定されない。例えば、コンテンツのタイトルが同じであれば、バージョンにかかわらず同じ鍵情報GKを用いるようにしてもかまわない。あるいは、同じコンテンツのタイトルに対して、出荷時期等を考慮して、定期的に鍵情報GKを変えるようにしてもよい。この場合、コンテンツ４１に当該コンテンツ４１の出荷時期がわかるような時期情報を入れておき、解除依頼にこの時期情報を含めて、ユーザ端末１から解除情報配信センタ２に送信する。そして、解除情報配信センタ２は、管理テーブル２１２において、鍵情報GKをコンテンツのタイトル名と時期情報とで管理することで、解除情報に含まれるコンテンツのタイトル名および時期情報から、当該解除情報に含まれる暗号文$C_{i,1}$を復号化するのに用いる鍵情報GKを、特定することができる。

【００９０】次に、本発明の第２実施形態について説明する。

【００９１】上記の第１実施形態では、ユーザ端末１は、解除情報配信センタ２に送信する解除情報に含まれる暗号文$C_{i,1}$を、鍵生成部１１１から受け取った鍵K_iとユーザの個人情報ID_iとを繋げたデータ（$K_i \| ID_i$）を鍵情報GK４２４を用いて暗号化することで作成している。このため、解除情報配信センタ２において、ユーザ認証を行う前の時点で、鍵K_iの内容が明らかになってしまう（図８のステップＳ１２０２、ステップＳ１２０３参照）。一方、解除情報配信センタ２は、ユーザ端末１に送信す暗号文$C_{i,2}$を、コンテンツ復号化のための鍵Kとユーザの個人情報ID_iとを繋げたデータ（$K \| ID_i$）を鍵K_iを用いて暗号化することで作成している。このため、ユーザ端末１において、ユーザ認証を行う前の時点で、鍵Kが取得されてしまう（図７のステップＳ１１０７、ステップＳ１１０８参照）。

【００９２】そこで、本実施形態では、解除情報配信センタ２において、ユーザ認証を行う前の時点で、鍵K_iの内容が明らかにならないように、多重に暗号化を施して暗号文$C_{i,1}$を作成すると共に、ユーザ端末１において、ユーザ認証を行う前の時点で、鍵Kの内容が明らかにならないように、多重に暗号化を施して暗号文$C_{i,2}$を作成するようにして、セキュリティを強化している。

【００９３】図１０は、本実施形態で用いられる記憶媒体４のデータ構成図である。

【００９４】ここで、図２に示す第１実施形態と同じ機能を有するものには、同じ符号を付している。図示するように、本実施形態では、利用制限解除プログラム４２に、共通鍵暗号体系に従った、コンテンツ４１に固有の３つの鍵情報$GK_1$４２４ａ、$GK_2$４２４ｂ、$GK_3$４２４ｃを格納している。

【００９５】なお、ユーザ端末１のハードウエア構成やソフトウエア構成は、図３および図４に示す第１実施形態ともと同様である。また、解除情報配信センタ２のハードウエア構成やソフトウエア構成も、基本的に第１実施形態のものと同様であるが、図１１に示すように、管理テーブル２１２に、タイトル名２１２ａおよびバージョン名２１２ｂにより特定されるコンテンツ４１に固有の３つの鍵情報$GK_1$２１２ｅ、$GK_2$２１２ｆ、$GK_3$２１

２ｇを格納している点が異なる。

【００９６】次に、本実施形態の動作について説明する。

【００９７】本実施形態の動作も、上記の第１実施形態と同様に、解除依頼生成処理、解除情報入手処理およびコンテンツ復号化処理の３つに分けられる。

【００９８】まず、解除依頼生成処理について説明する。

【００９９】図１２は、本実施形態の解除依頼生成処理を説明するための図である。

【０１００】ユーザ端末１において、主制御部１１４は、入力装置１５を介してユーザより解除依頼生成の指示を受け付けると、鍵生成部１１１に指示を出す。これを受けて、鍵生成部１１１は、乱数により鍵$K_{i,1}$、$K_{i,2}$を生成し、これを解除情報入手部１１２に渡す（ステップＳ２００１）。

【０１０１】次に、解除情報入手部１１２は、主制御部１１４を介して、フラッシュメモリ１３からユーザの個人情報ID_iを読み出すと共に、記憶媒体４から３つの鍵情報$GK_1$２１２ｅ、$GK_2$２１２ｆ、$GK_3$２１２ｇを読み出す。そして、共通鍵暗号体系にしたがい、鍵生成部１１１から受け取った鍵$K_{i,2}$を鍵情報$GK_3$２１２ｇで暗号化し、その結果$(E_{GK3}(K_{i,2}))$に鍵生成部１１１から受け取った鍵$K_{i,1}$を繋げたデータ$(E_{GK3}(K_{i,2})\|K_{i,1})$を、鍵情報$GK_2$２１２ｆでさらに暗号化する。そして、さらにその結果$(E_{GK2}(E_{GK3}(K_{i,2})\|K_{i,1}))$に、ユーザの個人情報$ID_i$を繋げたデータ$(E_{GK2}(E_{GK3}(K_{i,2})\|K_{i,1})\|ID_i)$を、$GK_1$２１２ｅで暗号化する。これにより、暗号文$C_{i,1}$（$=E_{GK1}(E_{GK2}(E_{GK3}(K_{i,2})\|K_{i,1})\|ID_i)$）を生成する（ステップＳ２００２）。

【０１０２】次いで、解除情報入手部１１２は、生成した暗号文$C_{i,1}$を、主制御部１１４を介してメモリカード２０に格納し（ステップＳ２００３）、その後、メモリ１２上のワークエリアから鍵$K_{i,1}$、$K_{i,2}$を除去して処理を終了する（ステップＳ２００４）。

【０１０３】次に、解除情報入手処理について説明する。

【０１０４】図１３および図１４は、本実施形態の解除情報入手処理を説明するための図であり、図１３はユーザ端末１側での処理を、そして、図１４は鍵情報配信センタ２側での処理を示している。

【０１０５】まず、ユーザ端末１において（図１３参照）、主制御部１１４は、入力装置１５を介してユーザより解除情報入手の指示を受け付けると、解除情報入手部１１２に指示を出す。これを受けて、解除情報入手部１１２は、主制御部１１４を介して、フラッシュメモリ１３からユーザの個人情報ID_iを読み出すと共に、記憶媒体４からコンテンツ４１のタイトルおよびバージョン名を読み出す。また、メモリカード２０から、解除依頼生成処理で作成した暗号文$C_{i,1}$（$=E_{GK1}(E_{GK2}(E_{GK3}(K_{i,2})\|K_{i,1})\|ID_i)$）を読み出す。そして、ユーザの個人情報$ID_i$とコンテンツのタイトルおよびバージョン名と暗号文$C_{i,1}$とを含んだ解除依頼を作成し（ステップＳ２１０１）、解除情報配信センタ２に送信する（ステップＳ２１０２）。

【０１０６】解除情報配信センタ２において（図１４参照）、解除情報送信部２１１は、ユーザ端末１より解除依頼を受信すると（ステップＳ２２０１）、管理テーブル２１２から、当該解除依頼に含まれているコンテンツのタイトルおよびバージョン名に対応する鍵情報$GK_3$２１２ｅ（これは当該コンテンツを格納する記憶媒体４の利用制限解除プログラム４２に格納されている鍵情報$GK_1$４２４ａと一致する）を読出し、この鍵情報GK_3を用いて、前記解除依頼に含まれている暗号文$C_{i,1}$を復号化する。これにより、ユーザの個人情報ID_iを得る（ステップＳ２２０２）。

【０１０７】それから、課金処理部２１３は、解除依頼を送信したユーザ端末１のユーザの認証を行う（ステップＳ２２０３）。例えば、受信した解除依頼に含まれているユーザの個人情報ID_iが正規のユーザとして記憶装置等に登録されているか否かを調べ、登録されているならば、当該個人情報ID_iとステップＳ１２０２で得たユーザの個人情報ID_iとを比較する。そして、両者が一致する場合は、ユーザ認証が成立したものとする。

【０１０８】ユーザ認証が成立しなかった場合（ステップＳ２２０４でＮｏ）は、その旨を解除情報送信部２１１に知らせて、前記解除依頼を送信したユーザ端末１にエラー通知を送信する（ステップＳ２２０５）。

【０１０９】一方、ユーザ認証が成立した場合（ステップＳ２２０４でＹｅｓ）は、そのユーザの個人情報ID_iにより特定されるユーザに対して課金処理を行い（ステップＳ２２０６）、その旨を解除情報送信部２１１に知らせる。解除情報送信部２１１は、管理テーブル２１２から、前記解除依頼に含まれているコンテンツのタイトルおよびバージョン名に対応する鍵情報$GK_2$２１２ｆ、$GK_3$２１２ｇ（これは当該コンテンツを格納する記憶媒体４の利用制限解除プログラム４２に格納されている鍵情報$GK_2$４２４ｂ、$GK_3$４２４ｃと一致する）を読出し、この鍵情報GK_2、GK_3を用いて、ステップＳ２２０２で暗号文$C_{i,1}$を復号化した結果得られたデータ$(E_{GK2}(E_{GK3}(K_{i,2})\|K_{i,1}))$を復号化する。これにより、鍵$K_{i,1}$、$K_{i,2}$を得る（ステップＳ２２０７）。

【０１１０】それから、解除情報送信部２１１は、管理テーブル２１２から、受信した解除依頼に含まれているコンテンツのタイトルおよびバージョン名に対応する鍵K２１２ｄ（これが当該タイトルおよびバージョン名により特定されるコンテンツ４１のアプリケーションデータ４１２の暗号化部分を復号化するための鍵（解除情報）である）を読出し、この鍵Kを前記鍵$K_{i,2}$で暗号化し、さらにその結果と前記ユーザの個人情報ID_iとを繋

げたデータ(E_{K12}(K)‖ID_U)を、前記鍵K_{11}で暗号化して、暗号文$C_{1,2}$（=E_{K11}(E_{K12}(K)‖ID_U)）を生成し（ステップＳ２２０８）、前記解除依頼を送信したユーザ端末１に送信する（ステップＳ２２０９）。

【０１１１】ユーザ端末１において（図１３参照）、解除情報入手部１１２は、解除情報配信センタ２より情報を受信すると（ステップＳ２１０３）、それがエラー通知ならば（ステップＳ２１０４でＮｏ）、その旨を本ユーザ端末１に接続されているテレビ等に出力するなど所定のエラー処理を行う（ステップＳ２１０５）。一方、暗号文$C_{1,2}$ならば（ステップＳ２１０４でＹｅｓ）、記憶媒体４から鍵情報$GK_1$４２４ａ、$GK_2$４２４ｂを読み出すと共に、メモリカード２０から、解除依頼生成処理で作成した暗号文$C_{1,1}$（=E_{GK1}(E_{GK2}(E_{GK3}(K_{12})‖K_{11})‖ID_U)）を読み出す。そして、この鍵情報GK_1、GK_2を用いて暗号文$C_{1,1}$を復号化し、ユーザの個人情報ID_Uと鍵K_{11}を得る（ステップＳ２１０６）。

【０１１２】次に、この鍵K_{11}を用いて、鍵情報配信センタ２より受信した暗号文$C_{1,2}$（=E_{K11}(E_{K12}(K)‖ID_U)）を復号化して、ユーザの個人情報ID_Uを得る（ステップＳ２１０７）。

【０１１３】それから、解除情報入手部１１２は、ステップＳ２１０６で暗号文$C_{1,1}$を復号化することで得たユーザの個人情報ID_Uと、ステップＳ２１０７で暗号文$C_{1,2}$を復号化することで得たユーザの個人情報ID_Uとを比較し、両者の一致を調べることで、ユーザ認証を行う（ステップＳ２１０８）。

【０１１４】ユーザ認証が成立しなかった場合（ステップＳ２１０９でＮｏ）は、その旨を本ユーザ端末１に接続されているテレビ等に出力するなど所定のエラー処理を行い、それから、メモリ１２上のワークエリアから鍵K_{11}、K_{12}を除去して処理を終了する（ステップＳ２１０５）。

【０１１５】一方、ユーザ認証が成立した場合（ステップＳ２１０９でＹｅｓ）は、鍵情報配信センタ２より受信した暗号文$C_{1,2}$を、主制御部１１４を介してメモリカード２０に、当該メモリカード２０に既に格納されている暗号文$C_{1,1}$と共に格納し（ステップＳ２１１０）、それから、メモリ１２上のワークエリアから鍵K_{11}、K_{12}を除去して処理を終了する（ステップＳ２１１１）。

【０１１６】次に、コンテンツ復号化処理について説明する。

【０１１７】図１５は、本実施形態のコンテンツ復号化処理を説明するための図である。

【０１１８】ユーザ端末１において、コンテンツ復号化部１１３は、アプリ処理部１１５によるアプリケーションデータ４１２の暗号化部分へのアクセスを監視する（ステップＳ２３０１）。そして、アプリ処理部１１５がアプリケーションデータ４１２の暗号化部分へアクセスし、主制御部１１４が暗号化データを読み出した場合には、これをフェッチする。

【０１１９】次に、コンテンツ復号化部１１３は、主制御部１１４を介して、メモリカード２０から暗号文$C_{1,1}$（=E_{GK1}(E_{GK2}(E_{GK3}(K_{12})‖K_{11})‖ID_U)）を読み出すと共に、記憶媒体４から鍵情報$GK_1$４２４ａを読出す。そして、この鍵情報GK_1を用いて暗号文$C_{1,1}$を復号化することにより、ユーザの個人情報ID_Uを得る（ステップＳ２３０２）。

【０１２０】それから、コンテンツ復号化部１１３は、主制御部１１４を介してフラッシュメモリ１３からユーザの個人情報ID_Uを読み出して、これとステップＳ２３０２で得たユーザの個人情報ID_Uとを比較し、両者の一致を調べることで、ユーザ認証を行う（ステップＳ２３０３）。

【０１２１】ユーザ認証が成立しなかった場合（ステップＳ２３０４でＮｏ）は、ステップＳ２３０１でフェッチした暗号化データをアプリ処理部１１５に渡し、その後、ステップＳ２３０１に戻る。

【０１２２】一方、ユーザ認証が成立した場合（ステップＳ２３０４でＹｅｓ）は、主制御部１１４を介して、記憶媒体４から鍵情報$GK_2$４２４ｂを読出す。そして、ステップＳ２３０２で暗号文$C_{1,1}$を復号化することにより得たデータ（(E_{GK2}(E_{GK3}(K_{12})‖K_{11})）を、この鍵情報GK_2で復号化し、鍵K_{11}を得る（ステップＳ２３０６）。また、主制御部１１４を介して、メモリカード２０から暗号文$C_{1,2}$（=E_{K11}(E_{K12}(K)‖ID_U)）を読み出し、これをステップＳ２３０６で得た鍵K_{11}を用いて復号化し、ユーザの個人情報ID_Uを得る（ステップＳ２３０７）。

【０１２３】それから、コンテンツ復号化部１１３は、ステップＳ２３０６で暗号文$C_{1,1}$を復号化することで得たユーザの個人情報ID_Uと、ステップＳ２３０６で暗号文$C_{1,2}$を復号化することで得たユーザの個人情報ID_Uとを比較し、両者の一致を調べることで、ユーザ認証を行う（ステップＳ２３０７）。

【０１２４】ユーザ認証が成立しなかった場合（ステップＳ２３０８でＮｏ）は、ステップＳ２３０１でフェッチした暗号化データをアプリ処理部１１５に渡し、その後、メモリ１２上のワークエリアから鍵K_{11}を除去してステップＳ２３０１に戻る。

【０１２５】一方、ユーザ認証が成立した場合（ステップＳ２３０８でＹｅｓ）は、主制御部１１４を介して、記憶媒体４から鍵情報$GK_3$４２４ｃを読出す。そして、ステップＳ２３０５での復号化により得たデータ（E_{GK3}(K_{12})）を、この鍵情報GK_3で復号化し、鍵K_{12}を得る（ステップＳ２３０９）。次に、この鍵K_{12}を用いて、ステップＳ２３０６で暗号文$C_{1,2}$を復号化することで得たデータ（E_{K12}(K)）を復号化し、鍵Kを得る（ステップＳ２３１０）。

【０１２６】それから、コンテンツ復号化部１１３は、

ステップＳ２３０１でフェッチした暗号化データを、ステップＳ２３１０で得た鍵Kを用いて復号化する（ステップＳ２３１１）。そして、復号化したデータをアプリ処理部１１５に渡した後、メモリ１２上のワークエリアから鍵K、K_{t1}、K_{t2}を除去して、ステップＳ２３０１に戻る。

【０１２７】以上、本発明の第２実施形態について説明した。

【０１２８】本実施形態によれば、解除情報配信センタ２において、ユーザ認証を行う前の時点で、鍵K_{t1}、K_{t2}の内容が明らかにならず、また、ユーザ端末１において、ユーザ認証を行う前の時点で、鍵Kの内容が明らかにならないので、セキュリティが向上する。

【０１２９】なお、本実施形態では、３つの鍵情報GK_1、GK_2、GK_3を用いて暗号文$C_{t,1}$（$=E_{GK1}(E_{GK2}(E_{GK3}(K_{t2}) \| K_{t1}) \| ID_t)$）を作成しているが、２つの鍵情報$GK_1$、$GK_2$を用いて暗号文$C_{t,1}$（$=E_{GK1}(E_{GK2}(K_{t2} \| K_{t1}) \| ID_t)$）を作成した場合でも、解除情報配信センタ２において、ユーザ認証を行う前の時点で鍵K_{t1}、K_{t2}の内容が明らかにならないようにすることができる。

【０１３０】次に、本発明の第３実施形態について説明する。

【０１３１】上記の第１、２実施形態では、記憶媒体４に格納するコンテンツの利用制限を暗号化により実現している。これに対し、本実施形態では、記憶媒体４に格納するコンテンツの利用制限をアクセス制御により実現している。そして、当該コンテンツの所定部分へアクセス禁止を解除するための認証情報（解除情報）を、上記の第１、２実施形態と同様に、共通鍵暗号体系に従った当該コンテンツに固有の鍵情報を用いた、暗号通信により、解除情報配信センタ２からユーザ端末１へ送信するようにしている。

【０１３２】図１６は、本実施形態で用いられる記憶媒体４のデータ構成図である。

【０１３３】ここで、図２に示す第１実施形態と同じ機能を有するものには、同じ符号を付している。図示するように、本実施形態では、アプリケーションデータ４１２は暗号化されていない。その代わり、アクセス制御プログラム４２５により、一部を除いて、アプリケーションプログラム４１１によるアプリケーションデータ４１２へのアクセスが禁止されている。認証情報AK４２６は、アプリケーションプログラム４１１によるアプリケーションデータ４１２のアクセス禁止領域へのアクセス禁止を解除するのに使用する情報であり、コンテンツ４１に固有の情報である。

【０１３４】図１７に、ユーザ端末１上に構築されるソフトウエア構成を示す。なお、ユーザ端末１のハードウエア構成は、第１実施形態のものと同様である。

【０１３５】本実施形態のユーザ端末１が図４に示す第１実施形態のものと異なる点は、コンテンツ復号化部１３に代えてアクセス制御部１１６が設けられている点である。アクセス制御部１１６は、アクセス制御プログラム４２５により実現される。解除情報入手部１１２で入手した解除情報（認証情報）と記憶媒体４に記憶されている認証情報AK４２６とを用いて、アプリケーションデータ４１２のアクセス禁止領域へのアクセスを制御する。

【０１３６】なお、解除情報配信センタ２のハードウエア構成やソフトウエア構成も、基本的に第１実施形態のものと同様であるが、図１８に示すように、管理テーブル２１２に、タイトル名２１２ａおよびバージョン名２１２ｂにより特定されるコンテンツ４１に固有の認証情報AK２１２ｈを格納している点が異なる。

【０１３７】次に、本実施形態の動作について説明する。

【０１３８】本実施形態の動作は、解除依頼生成処理、解除情報入手処理およびアクセス制御処理の３つに分けられる。このうち、解除依頼生成処理は図６に示す第１実施形態と同様である。また、解除情報入手処理も、暗号文$C_{t,2}$に含める解除情報が、解除依頼に含まれるコンテンツのタイトルおよびバージョンに対応する鍵K２１２ｄから認証情報AK２１２ｈに代わる点を除いて図７、図８に示すものと同じである。そこで、ここでは、アクセス制御処理についてのみ説明する。

【０１３９】図１９は、本実施形態のアクセス制御処理を説明するための図である。

【０１４０】ユーザ端末１において、アクセス制御部１１６は、アプリ処理部１１５によるアプリケーションデータ４１２のアクセス禁止部分へのアクセスを監視する（ステップＳ３３０１）。そして、アプリ処理部１１５が、アプリケーションデータ４１２のアクセス禁止部分へのアクセスを主制御部１１４に依頼した場合には、これをフェッチする。

【０１４１】次に、アクセス処理部１１６は、主制御部１１４を介して、メモリカード２０から暗号文$C_{t,1}$を読み出すと共に、記憶媒体４から鍵情報GK４２４を読出す。そして、この鍵情報GKを用いて暗号文$C_{t,1}$を復号化することにより、鍵K_tとユーザの個人情報ID_tを得る（ステップＳ３３０２）。

【０１４２】それから、アクセス処理部１１６は、主制御部１１４を介して、フラッシュメモリ１３からユーザの個人情報ID_tを読み出して、これとステップＳ３３０２で暗号文$C_{t,1}$を復号化することで得たユーザの個人情報ID_tとを比較し、両者の一致を調べることで、ユーザ認証を行う（ステップＳ３３０３）。

【０１４３】ユーザ認証が成立しなかった場合（ステップＳ３３０４でＮｏ）は、ステップＳ１３０１でフェッチした依頼を主制御部１１４に渡すことなく破棄し、その後、メモリ１２上のワークエリアから鍵K_tを除去してステップＳ３３０１に戻る。

【０１４４】一方、ユーザ認証が成立した場合（ステップＳ３３０４でＹｅｓ）は、主制御部１１４を介してメモリカード２０から暗号文$C_{1,2}$を読み出し、これをステップＳ３３０２で得た鍵K_1を用いて復号化し、認証情報AKとユーザの個人情報ID_1を得る（ステップＳ３３０５）。

【０１４５】それから、アクセス制御部１１６は、ステップＳ３３０２で暗号文$C_{1,1}$を復号化することで得たユーザの個人情報ID_1と、ステップＳ３３０５で暗号文$C_{1,2}$を復号化することで得たユーザの個人情報ID_1とを比較し、両者の一致を調べる。そして、両者が一致する場合は、主制御部１１４を介して記憶媒体４から認証情報AK４２６を読み出し、これと、ステップＳ３３０５で暗号文$C_{1,2}$を復号化することで得た認証情報AKとの一致を調べる。これにより、アクセス禁止部分へのアクセスを許可するか否かの認証を行う（ステップＳ３３０６）。

【０１４６】認証が成立しなかった場合（ステップＳ３３０７でＮｏ）は、ステップＳ３３０１でフェッチした依頼を主制御部１１４に渡すことなく破棄し、その後、メモリ１２上のワークエリアから認証情報AK、鍵K_1を除去して、ステップＳ３３０１に戻る。

【０１４７】一方、認証が成立した場合（ステップＳ３３０７でＹｅｓ）は、ステップＳ３３０１でフェッチした依頼を主制御部１１４に渡し、アプリ処理部１１５によるアプリケーションデータ４１２のアクセス禁止部分へのアクセスを許可する（ステップＳ３３０８）。その後、メモリ１２上のワークエリアから認証情報AK、鍵K_1を除去して、ステップＳ３３０１に戻る。

【０１４８】以上、本発明の第３実施形態について説明した。

【０１４９】本実施形態も、上記の第１実施形態と同様の効果を有する。加えて、本実施形態では、コンテンツの復号化処理を行うことなく、コンテンツの利用を制限しているので、ＣＰＵにかかる負荷をより低減できる。

【０１５０】なお、本実施形態においても、上記の第１実施形態と同様の変形が可能である。また、上記の第２実施形態と同様に、解除情報配信センタ２において、ユーザ認証を行う前の時点で、鍵K_1の内容が明らかにならないように、多重に暗号化を施して暗号文$C_{1,1}$を作成すると共に、ユーザ端末１において、ユーザ認証を行う前の時点で、認証情報AKの内容が明らかにならないように、多重に暗号化を施して暗号文$C_{1,1}$を作成するようにして、セキュリティを強化することもできる。

【０１５１】この場合、解除依頼生成処理は図１２に示す第２実施形態と同様である。また、解除情報入手処理も、暗号文$C_{1,2}$に含める解除情報が、解除依頼に含まれるコンテンツのタイトルおよびバージョンに対応する鍵K2１２ｄから認証情報AK２１２ｈに代わる点を除いて図１３、図１４に示すものと同じである。また、アクセス制御処理は、図１９に示すアクセス制御処理において、ステップＳ３３０２～ステップＳ３３０５に代えて図１５に示すステップＳ２３０２～Ｓ２３１０（但し、鍵Kに代えて認証情報AKとする）を採用したものとなる。

【０１５２】次に、本発明の第４実施形態について説明する。

【０１５３】本実施形態では、上記の第１実施形態と同様、記憶媒体４に格納するコンテンツの利用制限を暗号化により実現している。但し、当該コンテンツの暗号化部分を復号するための復号鍵（解除情報）を、ＲＳＡ暗号体系に従った当該コンテンツに固有の秘密鍵と公開鍵を用いた、暗号通信により、解除情報配信センタ２からユーザ端末１へ送信するようにしている。

【０１５４】まず、記憶媒体４のデータ構成について説明する。

【０１５５】図２０は、本実施形態で用いられる記憶媒体４のデータ構成図である。ここで、図２に示す第１実施形態のものと同じものには同じ符号を付している。

【０１５６】図示するように、本実施形態の利用制限解除プログラム４２は、解除情報入手プログラム４２７と、コンテンツ復号化プログラム４２３と、ＲＳＡ暗号体系に従った、コンテンツ４１に固有の公開鍵(n,e)４２９と、を有する。なお、ここでは、いわゆるバーションの相違も異なるコンテンツとみなしている。

【０１５７】図２１に、ユーザ端末１上に構築されるソフトウエア構成を示す。なお、ユーザ端末１のハードウエア構成は、第１実施形態のものと同様である。

【０１５８】本実施形態のユーザ端末１が図４に示す第１実施形態のものと異なる点は、鍵生成部１１１が省略されている点、および、解除情報入手部１１２に代えて解除情報入手部１１７が設けられている点である。解除情報入手部１１７は、解除情報入手プログラム４２７により実現され、記憶媒体４に格納されている公開鍵(n,e)４２９を用いて、解除情報配信センタ２より入手した暗号文を復号化し、コンテンツ復号化のための鍵K（解除情報）を入手する。

【０１５９】なお、解除情報配信センタ２のハードウエア構成やソフトウエア構成も、基本的に第１実施形態のものと同様であるが、図２２に示すように、管理テーブル２１２に、タイトル名２１２ａおよびバージョン名２１２ｂにより特定されるコンテンツ４１に固有の秘密鍵(n,d)２１２ｉ(当該コンテンツ４１に固有の公開鍵(n,e)４２９と対の鍵）を格納している点が異なる。また、解除情報送信部２１１に代えて解除情報送信部２１４を設けた点が異なる。解除情報送信部２１４は、コンテンツ復号化のための鍵K（解除情報）を含む情報を、秘密鍵(n,d)２１２ｉで暗号化し、ユーザ端末１へ送信する。

【０１６０】次に、本実施形態の動作について説明する。

【０１６１】本実施形態の動作は、ユーザ端末１が、解除依頼を鍵情報配信センタ２に送信して、鍵情報配信センタ２から鍵K（解除情報）を入手する解除情報入手処理、および、入手した鍵Kを用いてコンテンツ４１の暗号化部分を復号化するコンテンツ復号化処理の２つに分けられる。

【０１６２】まず、解除情報入手処理について説明する。

【０１６３】図２３および図２４は、本実施形態の解除情報入手処理を説明するための図であり、図２３はユーザ端末１側での処理を、そして、図２４は鍵情報配信センタ２側での処理を示している。

【０１６４】まず、ユーザ端末１において（図２３参照）、主制御部１１４は、入力装置１５を介してユーザより解除情報入手の指示を受け付けると、解除情報入手部１１７に指示を出す。これを受けて、解除情報入手部１１７は、主制御部１１４を介して、フラッシュメモリ１３からユーザの個人情報ID_uを読み出すと共に、記憶媒体４からコンテンツ４１のタイトルおよびバージョン名を読み出す。そして、ユーザの個人情報ID_uとコンテンツのタイトルおよびバージョン名とを含んだ解除依頼を作成し（ステップＳ４１０１）、解除情報配信センタ２に送信する（ステップＳ４１０２）。なお、ここで、個人情報ID_uは、セキュリティ強化のため、例えば記憶媒体４に格納されている公開鍵(n,e)４２９で暗号化しておくようにしてもよい。

【０１６５】解除情報配信センタ２において（図２４参照）、解除情報送信部２１４は、ユーザ端末１より解除依頼を受信すると（ステップＳ４２０１）、当該解除依頼に含まれているユーザの個人情報ID_uを課金処理部２１３に渡す。なお、個人情報個人情報ID_uが公開鍵(n,e)４２９で暗号化されている場合は、管理テーブル２１２に格納されている、当該解除依頼に含まれるコンテンツのタイトルおよびバージョン名に対応する秘密鍵（n,d）２１２ｉ（これは当該コンテンツを格納する記憶媒体４の利用制限解除プログラム４２に格納されている公開鍵(n,e)４２９と対の鍵である）で復号化してから、課金処理部２１３に渡す。

【０１６６】これを受けて、課金処理部２１３は、解除依頼を送信したユーザ端末１のユーザの認証を行う（ステップＳ４２０２）。例えば、解除情報送信部２１４より渡された解除依頼に含まれているユーザの個人情報ID_uが正規のユーザとして記憶装置等に登録されているか否かを調べ、登録されているならば、ユーザ認証が成立したものとする。

【０１６７】ユーザ認証が成立しなかった場合（ステップＳ４２０３でＮｏ）は、その旨を解除情報送信部２１４に知らせて、前記解除依頼を送信したユーザ端末１にエラー通知を送信する（ステップＳ４２０４）。

【０１６８】一方、ユーザ認証が成立した場合（ステップＳ４２０３でＹｅｓ）は、そのユーザの個人情報ID_uにより特定されるユーザに対して課金処理を行い（ステップＳ４２０５）、その旨を解除情報送信部２１４に知らせる。解除情報送信部２１４は、管理テーブル２１２から、受信した解除依頼に含まれているコンテンツのタイトルおよびバージョン名に対応する秘密鍵（n,d)２１２ｉと鍵K２１２ｄを読出し、この鍵Kと前記ユーザの個人情報ID_uとを繋げたデータ（K‖ID_u）を、秘密鍵（n,d）で暗号化して、暗号文$C_{1,2}$（$=(K \| ID_u)^d \bmod n$）を生成し（ステップＳ４２０６）、前記解除依頼を送信したユーザ端末１に送信する（ステップＳ４２０７）。

【０１６９】ユーザ端末１において（図２３参照）、解除情報入手部１１７は、解除情報配信センタ２より情報を受信すると（ステップＳ４１０３）、それがエラー通知ならば（ステップＳ４１０４でＮｏ）、その旨を本ユーザ端末１に接続されているテレビ等に出力するなど所定のエラー処理を行う（ステップＳ４１０５）。一方、暗号文$C_{1,2}$ならば（ステップＳ４１０４でＹｅｓ）、記憶媒体４から公開鍵(n,e)４２９を読み出す。そして、この公開鍵(n,e)を用いて暗号文$C_{1,2}$を復号化し（$=C_{1,2}{}^{e} \bmod n$）、コンテンツ４１復号化のための鍵Kとユーザの個人情報ID_uを得る（ステップＳ４１０６）。

【０１７０】それから、解除情報入手部１１７は、ステップＳ４１０６で得たユーザの個人情報ID_uを、フラッシュメモリ１３より読み出したユーザの個人情報ID_uと比較し、両者の一致を調べることで、ユーザ認証を行う（ステップＳ４１０７）。

【０１７１】ユーザ認証が成立しなかった場合（ステップＳ４１０８でＮｏ）は、その旨を本ユーザ端末１に接続されているテレビ等に出力するなど所定のエラー処理を行うと共に、メモリ１２上のワークエリアから復号結果を除去する（ステップＳ４１０５）。

【０１７２】一方、ユーザ認証が成立した場合（ステップＳ４１０８でＹｅｓ）は、鍵情報配信センタ２より受信した暗号文$C_{1,2}$を、主制御部１１４を介してメモリカード２０に格納すると共に、メモリ１２上のワークエリアから復号結果を除去する（ステップＳ４１０９）。

【０１７３】次に、コンテンツ復号化処理について説明する。

【０１７４】図２５は、本実施形態のコンテンツ復号化処理を説明するための図である。

【０１７５】ユーザ端末１において、コンテンツ復号化部１１３は、アプリ処理部１１５によるアプリケーションデータ４１２の暗号化部分へのアクセスを監視する（ステップＳ４３０１）。そして、アプリ処理部１１５がアプリケーションデータ４１２の暗号化部分へアクセスし、主制御部１１４が暗号化データを読み出した場合には、これをフェッチする。

【０１７６】次に、コンテンツ復号化部１１３は、主制御部１１４を介して、メモリカード２０から暗号文$C_{1,2}$

を読み出すと共に、記憶媒体４から公開鍵(n,e)４２９を読出す。そして、この公開鍵(n,e)を用いて暗号文$C_{1,2}$を復号化することにより、鍵Kとユーザの個人情報ID_uを得る（ステップＳ４３０２）。

【０１７７】それから、コンテンツ復号化部１１３は、主制御部１１４を介してフラッシュメモリ１３からユーザの個人情報ID_uを読み出して、これとステップＳ４３０２で得たユーザの個人情報ID_uとを比較し、両者の一致を調べることで、ユーザ認証を行う（ステップＳ４３０３）。

【０１７８】ユーザ認証が成立しなかった場合（ステップＳ４３０４でＮｏ）は、ステップＳ４３０１でフェッチした暗号化データをアプリ処理部１１５に渡し、その後、メモリ１２上のワークエリアから鍵Kを除去して、ステップＳ４３０１に戻る。

【０１７９】一方、ユーザ認証が成立した場合（ステップＳ４３０４でＹｅｓ）は、ステップＳ４３０１でフェッチした暗号化データを、ステップＳ４３０２で得た鍵Kを用いて復号化する（ステップＳ４３０５）。そして、復号化したデータをアプリ処理部１１５に渡した後、メモリ１２上のワークエリアから鍵Kを除去して（ステップ４３０６）、ステップＳ４３０１に戻る。

【０１８０】以上、本発明の第４実施形態について説明した。

【０１８１】本実施形態においても、上記の第１実施形態と同様、同じコンテンツ４１であれば、当該コンテンツ４１と共に記録媒体４に記憶する公開鍵(n,e)４２９も同じものになるので、つまり、記憶媒体４毎に固有の情報を当該記憶媒体４に記憶させる必要がないので、当該記憶媒体４を例えばプレス等により大量生産するのに好適である。

【０１８２】加えて、本実施形態によれば、記憶媒体４に記憶される鍵を、ＲＳＡ暗号体系に従った公開鍵(n,e)としている。つまり、当該鍵からは解除情報配信センタ２が保持する対の秘密鍵(n,d)を推測不可能な鍵としている。したがって、例えば不正な第３者が記憶媒体４の内容を解析して公開鍵(n,e)を入手したとしても、当該鍵からこれと対の秘密鍵(n,d)を求めることができない以上、当該第３者が、前記公開鍵(n,e)で復号可能な解除情報（鍵K）を含む暗号文$C_{1,2}$を生成することはできない。つまり、当該第３者が解除情報配信センタの運営者になりすまして、解除情報配信サービスの提供を行うのを防ぐことができる。

【０１８３】なお、上記の第４実施形態では、解除情報配信センタ２がユーザ端末１に送信する暗号文$C_{1,2}$を、コンテンツ復号化のための鍵Kとユーザの個人情報ID_uとを繋げたデータ（K‖ID_u）を秘密鍵(n,d)２１２ｉで暗号化することで作成している。しかしながら、鍵Kとユーザの個人情報ID_uにその他のデータを繋げたデータを秘密鍵(n,d)で暗号化することで、暗号文$C_{1,2}$を作成するようにしてもよい。例えば解除情報送信部２１４に乱数Rを生成させ、鍵Kとユーザの個人情報ID_uと乱数Rを繋げたデータ（K‖ID_u‖R）を、秘密鍵（n,d)で暗号化することで、暗号文$C_{1,2}$を(=（K‖ID_u‖R）^{d} mod n)作成するようにしてもよい。このようにすれば、暗号文$C_{1,2}$から鍵Kが不正に解読される可能性をより低くできる。

【０１８４】また、上記の第４実施形態では、コンテンツのタイトルのみならずバージョンが異なる場合でも、秘密鍵（n,d)と公開鍵(n,e)の対が異なるようにしているが、これに限定されない。例えば、コンテンツのタイトルが同じであれば、バージョンにかかわらず同じ秘密鍵（n,d)と公開鍵(n,e)の対を用いるようにしてもかまわない。あるいは、同じコンテンツのタイトルに対して、出荷時期等を考慮して、定期的に秘密鍵（n,d)と公開鍵(n,e)の対を変えるようにしてもよい。この場合、コンテンツ４１に当該コンテンツ４１の出荷時期がわかるような時期情報を入れておき、解除依頼にこの時期情報を含めて、ユーザ端末１から解除情報配信センタ２に送信する。そして、解除情報配信センタ２は、管理テーブル２１２において、秘密鍵（n,d)をコンテンツのタイトル名と時期情報とで管理することで、解除情報に含まれるコンテンツのタイトル名および時期情報から秘密鍵（n,d)を特定することができる。

【０１８５】次に、本発明の第５実施形態について説明する。

【０１８６】上記の第４実施形態では、解除情報配信センタ２は、ユーザ端末１に送信す暗号文$C_{1,2}$を、コンテンツ復号化のための鍵Kとユーザの個人情報ID_uとを繋げたデータ（K‖ID_u)を秘密鍵（n,d)を用いて暗号化することで作成している。このため、ユーザ端末１において、ユーザ認証を行う前の時点で、鍵Kが取得されてしまう（図２３のステップＳ４１０６、ステップＳ４１０７参照）。

【０１８７】そこで、本実施形態では、ユーザ端末１において、ユーザ認証を行う前の時点で、鍵Kの内容が明らかにならないように、多重に暗号化を施して暗号文$C_{1,2}$を作成するようにして、セキュリティを強化している。

【０１８８】図２６は、本実施形態で用いられる記憶媒体４のデータ構成図である。

【０１８９】ここで、図２０に示す第４実施形態と同じ機能を有するものには、同じ符号を付している。図示するように、本実施形態では、利用制限解除プログラム４２に、ＲＳＡ暗号体系に従った、コンテンツ４１に固有の２つの公開鍵(n_1,e_1)４２９ａ、(n_2,e_2)４２９ｂを格納している。

【０１９０】なお、ユーザ端末１のハードウエア構成やソフトウエア構成は、第４実施形態のものと同様である。また、解除情報配信センタ２のハードウエア構成やソフトウエア構成も、基本的に第４実施形態のものと同

様であるが、図２７に示すように、管理テーブル２１２に、タイトル名２１２ａおよびバージョン名２１２ｂにより特定されるコンテンツ４１に固有の、ＲＳＡ暗号体系に従った２つの秘密鍵（n_1,d_1）２１２ｊ、（n_2,d_2）２１２ｋを格納している点が異なる。

【０１９１】次に、本実施形態の動作について説明する。

【０１９２】本実施形態の動作も、上記の第４実施形態と同様に、解除情報入手処理およびコンテンツ復号化処理の２つに分けられる。

【０１９３】まず、解除情報入手処理について説明する。

【０１９４】図２８および図２９は、本実施形態の解除情報入手処理を説明するための図であり、図２８はユーザ端末１側での処理を、そして、図２９は鍵情報配信センタ２側での処理を示している。

【０１９５】まず、ユーザ端末１において（図２８参照）、主制御部１１４は、入力装置１５を介してユーザより解除情報入手の指示を受け付けると、解除情報入手部１１７に指示を出す。これを受けて、解除情報入手部１１７は、主制御部１１４を介して、フラッシュメモリ１３からユーザの個人情報ID_uを読み出すと共に、記憶媒体４からコンテンツ４１のタイトルおよびバージョン名を読み出す。そして、ユーザの個人情報ID_uとコンテンツのタイトルおよびバージョン名とを含んだ解除依頼を作成し（ステップＳ５１０１）、解除情報配信センタ２に送信する（ステップＳ５１０２）。なお、ここで、個人情報ID_uは、セキュリティ強化のため、例えば記憶媒体４に格納されている公開鍵（n_1,e_1）４２９ａで暗号化しておくようにしてもよい。

【０１９６】解除情報配信センタ２において（図２９参照）、解除情報送信部２１４は、ユーザ端末１より解除依頼を受信すると（ステップＳ５２０１）、当該解除依頼に含まれているユーザの個人情報ID_uを課金処理部２１３に渡す。なお、個人情報個人情報ID_uが公開鍵（n_1,e_1）４２９ａで暗号化されている場合は、管理テーブル２１２に格納されている、当該解除依頼に含まれるコンテンツのタイトルおよびバージョン名に対応する秘密鍵（n_1,d_1）２１２ｊ（これは当該コンテンツを格納する記憶媒体４の利用制限解除プログラム４２に格納されている公開鍵（n_1,e_1）４２９ａと対の鍵である）で復号化してから、課金処理部２１３に渡す。

【０１９７】これを受けて、課金処理部２１３は、解除依頼を送信したユーザ端末１のユーザの認証を行う（ステップＳ５２０２）。例えば、解除情報送信部２１４より渡された解除依頼に含まれているユーザの個人情報ID_uが正規のユーザとして記憶装置等に登録されているか否かを調べ、登録されているならば、ユーザ認証が成立したものとする。

【０１９８】ユーザ認証が成立しなかった場合（ステップＳ５２０３でＮｏ）は、その旨を解除情報送信部２１４に知らせて、前記解除依頼を送信したユーザ端末１にエラー通知を送信する（ステップＳ５２０４）。

【０１９９】一方、ユーザ認証が成立した場合（ステップＳ５２０３でＹｅｓ）は、そのユーザの個人情報ID_uにより特定されるユーザに対して課金処理を行い（ステップＳ５２０５）、その旨を解除情報送信部２１４に知らせる。解除情報送信部２１４は、管理テーブル２１２から、解除依頼に含まれているコンテンツのタイトルおよびバージョン名に対応する秘密鍵（n_1,d_1）２１２ｊ、（n_2,d_2）２１２ｊと、鍵Ｋ２１２ｄを読出す。そして、この鍵Ｋを秘密鍵（n_2,d_2）で暗号化し、その暗号結果（$K^{d_2} \bmod n_2$）とユーザの個人情報ID_uとを繋げたデータ（$(K^{d_2} \bmod n_2) \| ID_u$）を、秘密鍵（$n_1$,$d_1$）でさらに暗号化して、暗号文$C_{1,2}$（$=((K^{d_2} \bmod n_2) \| ID_u)^{d_1} \bmod n_1$）を生成し（ステップＳ５２０６）、前記解除依頼を送信したユーザ端末１に送信する（ステップＳ５２０７）。

【０２００】ユーザ端末１において（図２８参照）、解除情報入手部１１７は、解除情報配信センタ２より情報を受信すると（ステップＳ５１０３）、それがエラー通知ならば（ステップＳ５１０４でＮｏ）、その旨を本ユーザ端末１に接続されているテレビ等に出力するなど所定のエラー処理を行う（ステップＳ５１０５）。一方、暗号文$C_{1,2}$ならば（ステップＳ５１０４でＹｅｓ）、記憶媒体４から公開鍵（n_1,e_1）４２９ａを読み出す。そして、この公開鍵（n_1,e_1）を用いて暗号文$C_{1,2}$を復号化し（$=C_{1,2}^{e_1} \bmod n_1$）、ユーザの個人情報ID_uを得る（ステップＳ５１０６）。

【０２０１】それから、解除情報入手部１１７は、ステップＳ５１０６で得たユーザの個人情報ID_uを、フラッシュメモリ１３より読み出したユーザの個人情報ID_uと比較し、両者の一致を調べることで、ユーザ認証を行う（ステップＳ５１０７）。

【０２０２】ユーザ認証が成立しなかった場合（ステップＳ５１０８でＮｏ）は、その旨を本ユーザ端末１に接続されているテレビ等に出力するなど所定のエラー処理を行うと共に、メモリ１２上のワークエリアから復号結果を除去する（ステップＳ５１０５）。

【０２０３】一方、ユーザ認証が成立した場合（ステップＳ５１０８でＹｅｓ）は、鍵情報配信センタ２より受信した暗号文$C_{1,2}$を、主制御部１１４を介してメモリカード２０に格納すると共に、メモリ１２上のワークエリアから復号結果を除去する（ステップＳ５１０９）。

【０２０４】次に、コンテンツ復号化処理について説明する。

【０２０５】図３０は、本実施形態のコンテンツ復号化処理を説明するための図である。

【０２０６】ユーザ端末１において、コンテンツ復号化部１１３は、アプリ処理部１１５によるアプリケーショ

ンデータ４１２の暗号化部分へのアクセスを監視する（ステップＳ５３０１）。そして、アプリ処理部１１５がアプリケーションデータ４１２の暗号化部分へアクセスし、主制御部１１４が暗号化データを読み出した場合には、これをフェッチする。

【０２０７】次に、コンテンツ復号化部１１３は、主制御部１１４を介して、メモリカード２０から暗号文$C_{1,2}$を読み出すと共に、記憶媒体４から公開鍵(n_1, e_1)４２９ａを読出す。そして、この公開鍵(n_1, e_1)を用いて暗号文$C_{1,2}$を復号化することにより、ユーザの個人情報ID_uを得る（ステップＳ５３０２）。

【０２０８】それから、コンテンツ復号化部１１３は、主制御部１１４を介してフラッシュメモリ１３からユーザの個人情報ID_uを読み出して、これとステップＳ５３０２で得たユーザの個人情報ID_uとを比較し、両者の一致を調べることで、ユーザ認証を行う（ステップＳ５３０３）。

【０２０９】ユーザ認証が成立しなかった場合（ステップＳ５３０４でＮｏ）は、ステップＳ５３０１でフェッチした暗号化データをアプリ処理部１１５に渡し、ステップＳ５３０１に戻る。

【０２１０】一方、ユーザ認証が成立した場合（ステップＳ５３０４でＹｅｓ）は、主制御部１１４を介して、記憶媒体４から公開鍵(n_2, e_2)４２９ｂを読出す。そして、この公開鍵(n_2, e_2)を用いて、ステップＳ５３０２にて暗号文$C_{1,2}$を復号化するこで得たデータ$(K^{e_2} \bmod n_2)$を復号化し、鍵Ｋを得る（ステップＳ５３０５）。そして、この鍵Ｋを用いて、ステップＳ５３０１でフェッチした暗号化データを復号化し（ステップＳ５３０６）、復号化したデータをアプリ処理部１１５に渡した後、メモリ１２上のワークエリアから鍵Ｋを除去して（ステップ５３０７）、ステップＳ５３０１に戻る。

【０２１１】以上、本発明の第５実施形態について説明した。

【０２１２】本実施形態によれば、ユーザ端末１において、ユーザ認証を行う前の時点で、鍵Ｋの内容が明らかにならないので、セキュリティが向上する。

【０２１３】なお、上記の第４、５実施形態では、コンテンツ復号化のための鍵Ｋ（解除情報）を、ＲＳＡ暗号を利用して解除情報配信センタ２からユーザ端末１へ送信するようにしているが、解除情報配信センタ２が保持する鍵（暗号鍵）が、ユーザ端末１が保持する前記鍵と対の鍵（復号鍵）からは推測不可能な非対称暗号を利用するものであれば、どのようなものであってもかまわない。

【０２１４】また、上記の第４、５実施形態では、記憶媒体４に格納するコンテンツの利用制限を暗号化により実現しているが、これらの実施形態を、上記の第３実施形態と同様に、記憶媒体４に格納するコンテンツの利用制限をアクセス制御により実現することも可能である。つまり、上記の第３、４実施形態において、コンテンツ復号化のための鍵Ｋに代えて、コンテンツのアクセス禁止を解除するための認証情報ＡＫを解除情報配信センタ２からユーザ端末１へ送信し、ユーザ端末１で、この受信した認証情報ＡＫと記憶媒体４に記憶されている認証情報ＡＫとの一致を調べることで、アクセス禁止を解除するか否か判断することも可能である。

【０２１５】以上、本発明の各実施形態について説明した。

【０２１６】本発明は、上記の各実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

【０２１７】たとえば、上記の各実施形態において、利用制御解除プログラム４２は、コンテンツ４１のアプリケーションプログラム４１１の１部として組み込まれたものであってもかまわない。また、セキュリティ強化のため、利用制御解除プログラム４２中の各プログラムが用いる暗号アルゴリズムは公開しない方が好ましい。

【０２１８】また、解除依頼のユーザ端末１から解除情報配信センタへの送信、および、解除情報の解除情報配信センタ２からユーザ端末１への送信は、上記の各実施形態のものに限定されるものではない。ネットワーク３上でのセキュリティが確保される方法によるものであれば、どのようなものであってもかまわない。

【０２１９】また、上記の第１、２、４および５実施形態では、コンテンツ４１の１部を暗号化することでその利用を制限し、コンテンツ４１の暗号化部分を復号化するための鍵Ｋを解除情報としている。また、上記の第３実施形態では、コンテンツ４１の１部へのアクセスを禁止することでその利用を制限し、コンテンツ４１のアクセス禁止部分へのアクセスを許可するための認証情報ＡＫを解除情報としている。しかしながら、本発明はこれに限定されない。

【０２２０】本発明は、何らかの方法によりコンテンツの利用が制限されており、そのアクセス制限を解除するための情報が、ユーザ端末１による解除依頼に従い、解除情報配信センタ２からユーザ端末１へ送信されるものであればよい。

【０２２１】たとえば、図３１に示すように、解除情報としてデジタル署名を用い、ユーザ端末１において、前記デジタル署名の検証を行い、その正当性が成立した場合にコンテンツ４１の利用制限を解除するようにしてもよい。

【０２２２】なお、図３１に示す例では、ユーザ端末１は、乱数、時刻情報、ユーザの個人情報ID_u、あるいは、コンテンツ４１の識別情報、もしくは、これらの情報のうちの少なくとも２つの組み合わせでなる任意の情報Ｍを、解除依頼に含めて送信する（Ｓ６００１）。これを受けて、解除情報配信センタ２は、コンテンツ４１の利用制限の解除を許可する場合、例えばコンテンツ４

１毎に固有の秘密鍵SKを用いて、前記解除情報に含まれる情報Mに対するデジタル署名sgnを生成し（Ｓ６００２）、ユーザ端末１に送信する（Ｓ６００３）。ユーザ端末１は、例えば記憶媒体４に格納されているコンテンツ４１に固有の（秘密鍵SKと対の）公開鍵PKを用いて、デジタル署名sgnを検証し（Ｓ６００４）、当該署名の正当性が確認できた場合にのみ、メモリカード２０等に格納する（Ｓ６００５）。そして、ユーザ端末１は、コンテンツ４１の利用制限部分にアクセスする都度、メモリカード２０等からデジタル署名sgnを読み出して検証し、当該署名の正当性が確認できた場合にのみ、コンテンツ４１の利用制限部分へのアクセスを許可する。

【０２２３】このようにした場合、ユーザ端末１は、デジタル署名sgnの正当性が確認できた場合にのみ、つまり、解除情報配信センタ２がコンテンツ４１の利用制限の解除を許可していることが正しく確認できた場合にのみ、ユーザにコンテンツ４１の利用制限部分の利用を許可することができる。

【０２２４】なお、解除情報配信センタ２における、コンテンツ４１の利用制限の解除を許可するか否かの判断は、例えば図３１に示す処理に先だって行われた、ユーザ認証処理や課金処理等での結果に基づいて行うようにしてもよい。あるいは、解除依頼中の情報Mにユーザの個人情報ID_uが含まれている場合、この個人情報ID_uが正規のユーザとして解除情報配信センタ２に登録されているか否かを調べることで行うようにしてもよい。また、ユーザ端末１側での処理を行うために必要なプログラム（解除依頼生成・送信のためのプログラムや署名検証ためのプログラムやコンテンツ４１へのアクセスを制御するためのプログラム等）やデータ（コンテンツ４１に固有の公開鍵PK等）は、上記の第１～第５実施形態と同様、コンテンツ４１と共に記憶媒体４に格納しておくようにすればよい。

【０２２５】また、上記の各実施形態において、各種認証にユーザの個人情報ID_uを用いているが、当該情報の代わりに、ユーザ端末１のフラッシュメモリ１３等に格納されているユーザ端末に固有の識別情報ID_tを用いるようにしても構わない。なお、上記の各実施形態において、ユーザ端末１にダウンロードされた解除情報（鍵Kや認証情報AK）はメモリカード２０に格納されるが、上記の各実施形態では、ユーザ端末１のフラッシュメモリ１３等に識別情報IDを格納し、この識別情報IDを用いて認証を行うことで、メモリーカード２０に格納された解除情報が不正にコピーされたり、あるいは、このメモリーカード２０が他の課金されていないユーザ端末１に装着されたりして、コンテンツが不正に使用可能となるのを防止している。

【０２２６】また、上記の各実施形態では、ユーザ端末１のフラッシュメモリ１３に、予めＯＳを格納するようにしている。しかし、ユーザ端末１が記録媒体４からブート可能に構成されている場合は、当該ＯＳを記録媒体４に格納するようにしてもよい。なお、記録媒体４に格納されている各種プログラムが、ＯＳプログラムを介さずに、直接、ユーザ端末１を各部を制御できる場合（いわゆるＯＳレス環境）、フラッシュメモリ１３に予めＯＳプログラムを格納しておく必要はない。

【０２２７】また、上記の各実施形態では、ユーザ端末１での解除情報入手処理において、解除情報のメモリカード２０への記録に先立ち認証を行っている。しかし、これは省略してもよい。この場合でも、ユーザ端末１でのコンテンツ復号化処理あるいはアクセス制御処理において認証を行っているので、コンテンツの不正な使用を制限できる。

【０２２８】

【発明の効果】以上説明したように、本発明によれば、ユーザに過度の負担をかけることなく、コンテンツの正規購入に先だってそのコンテンツを評価できるようにすることが可能となる。

【図面の簡単な説明】

【図１】本発明の各実施形態が適用されるコンテンツ利用制限解除システムの概略構成図である。

【図２】本発明の第１実施形態で用いられる記憶媒体４のデータ構成図である。

【図３】図１に示すユーザ端末１のハードウエア構成の一例を示す図である。

【図４】本発明の第１実施形態において、ユーザ端末１上に構築されるソフトウエア構成を示す図である。

【図５】本発明の第１実施形態において、解除情報配信センタ２上に構築されるソフトウエア構成を示す図である。

【図６】本発明の第１実施形態における解除依頼生成処理を説明するための図である。

【図７】本発明の第１実施形態における解除情報入手処理（ユーザ端末１側）を説明するための図である。

【図８】本発明の第１実施形態における解除情報入手処理（鍵情報配信センタ２側）を説明するための図である。

【図９】本発明の第１実施形態におけるコンテンツ復号化処理を説明するための図である。

【図１０】本発明の第２実施形態で用いられる記憶媒体４のデータ構成図である。

【図１１】本発明の第２実施形態において、解除情報配信センタ２上に構築されるソフトウエア構成を示す図である。

【図１２】本発明の第２実施形態における解除依頼生成処理を説明するための図である。

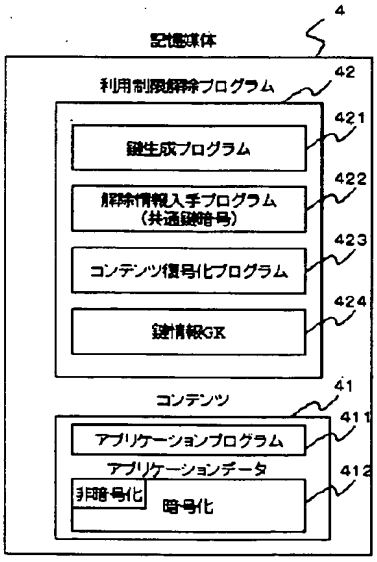
【図１３】本発明の第２実施形態における解除情報入手処理（ユーザ端末１側）を説明するための図である。

【図１４】本発明の第２実施形態における解除情報入手処理（鍵情報配信センタ２側）を説明するための図であ

る。
【図１５】本発明の第２実施形態のコンテンツ復号化処理を説明するための図である。
【図１６】本発明の第３実施形態で用いられる記憶媒体４のデータ構成図である。
【図１７】本発明の第３実施形態において、ユーザ端末１上に構築されるソフトウエア構成を示す図である。
【図１８】本発明の第３実施形態において、解除情報配信センタ２上に構築されるソフトウエア構成を示す図である。
【図１９】本発明の第３実施形態におけるアクセス制御処理を説明するための図である。
【図２０】本発明の第４実施形態で用いられる記憶媒体４のデータ構成図である。
【図２１】本発明の第４実施形態において、ユーザ端末１上に構築されるソフトウエア構成を示す図である。
【図２２】本発明の第４実施形態において、解除情報配信センタ２上に構築されるソフトウエア構成を示す図である。
【図２３】本発明の第４実施形態における解除情報入手処理（ユーザ端末１側）を説明するための図である。
【図２４】本発明の第４実施形態における解除情報入手処理（鍵情報配信センタ２側）を説明するための図である。
【図２５】本発明の第４実施形態のコンテンツ復号化処理を説明するための図である。
【図２６】本発明の第５実施形態で用いられる記憶媒体＊４のデータ構成図である。
【図２７】本発明の第５実施形態において、解除情報配信センタ２上に構築されるソフトウエア構成を示す図である。
【図２８】本発明の第５実施形態における解除情報入手処理（ユーザ端末１側）を説明するための図である。
【図２９】本発明の第５実施形態における解除情報入手処理（鍵情報配信センタ２側）を説明するための図である。
【図３０】本発明の第５実施形態におけるコンテンツ復号化処理を説明するための図である。
【図３１】本発明において、デジタル署名を利用して、コンテンツ４１の利用制限を解除するようにした場合の処理の流れを説明するための図である。
【符号の説明】
１…ユーザ端末、　２…解除情報配信センタ、　３…ネットワーク、　４…記憶媒体、　１１…ＣＰＵ、　１２…メモリ、　１３…フラッシュメモリ、　１４…通信装置、　１５…入力装置、　１６…オーディオ再生装置、　１７…ビデオ再生装置、　１８…カード接続装置、１９…読取装置　２０…メモリカード、２１…インターフェース、４１…コンテンツ、　４２…　利用制御解除プログラム、　１１１…鍵生成部、　１１２,１１７…解除情報入手部、　１１３…コンテンツ復号化部、　１１４…主制御部、　１１５…アプリ処理部、１１６…アクセス制御部、　２１１,２１４…解除情報送信部、　２１２…管理テーブル、２１３…課金処理部

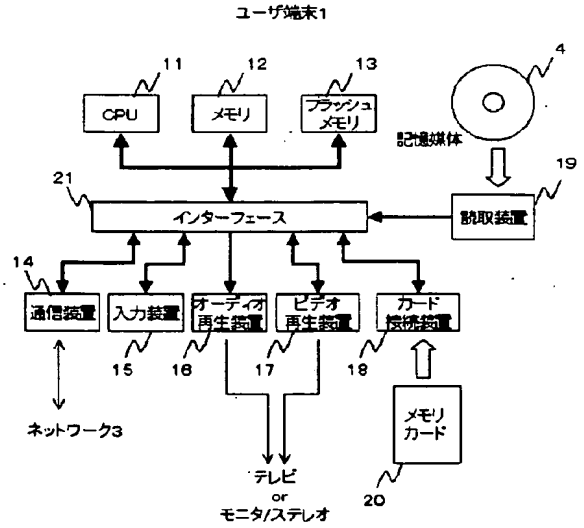
【図２】

図2



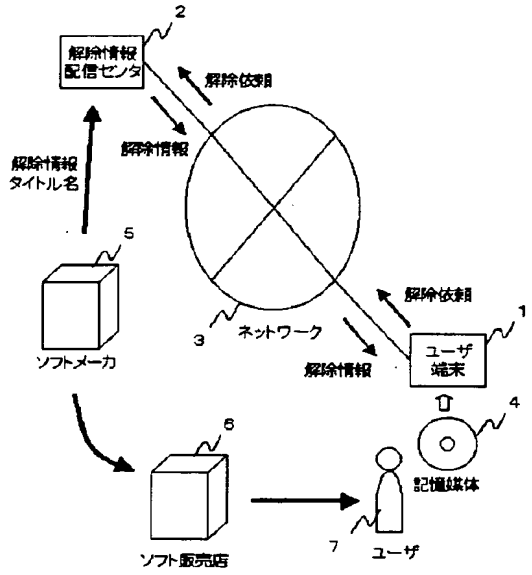
【図３】

図3



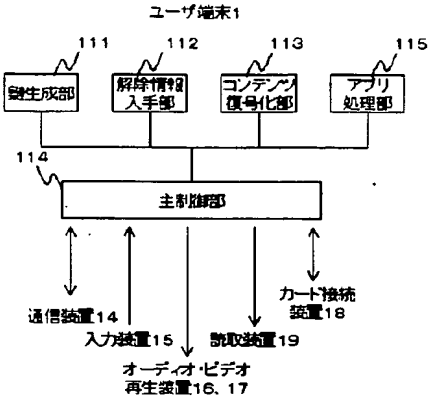
【図１】

図1



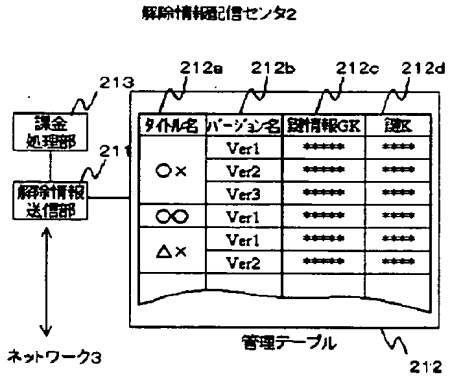
【図４】

図4



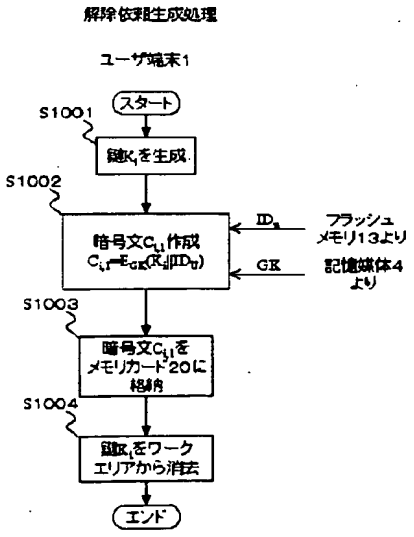
【図５】

図5



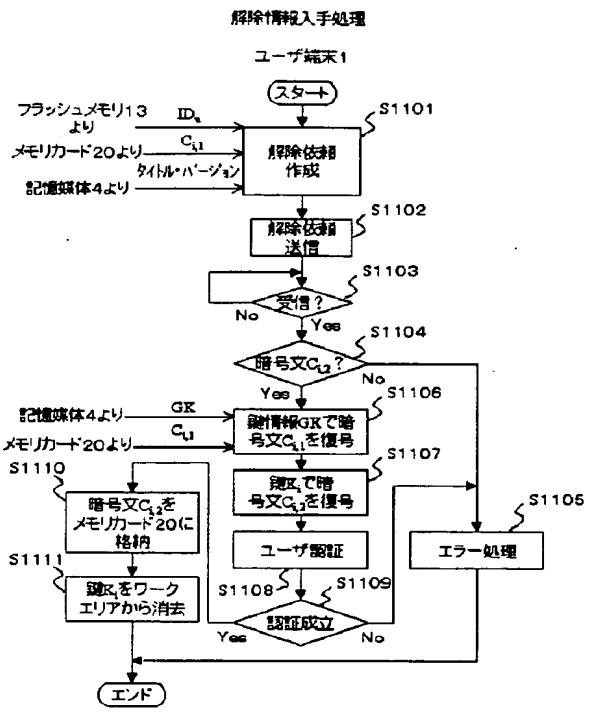
【図６】

図6



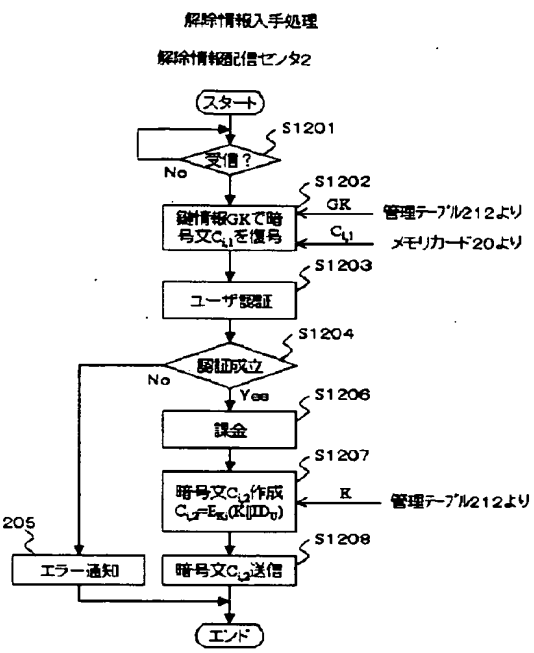
【図７】

図7



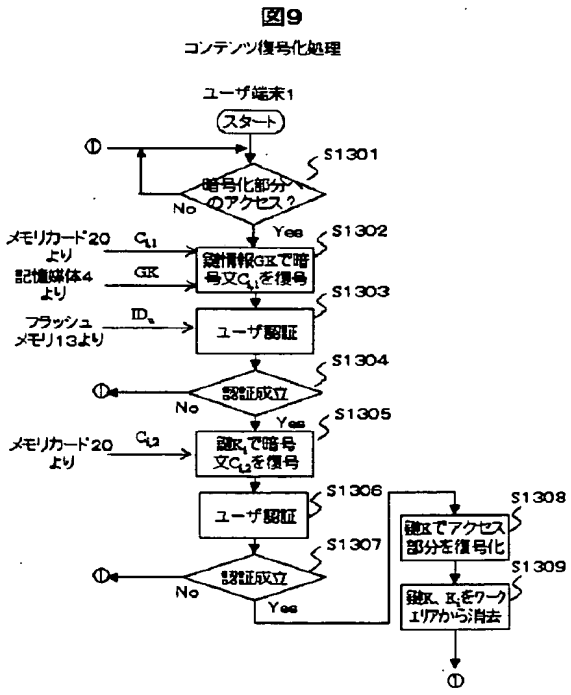
【図８】

図8



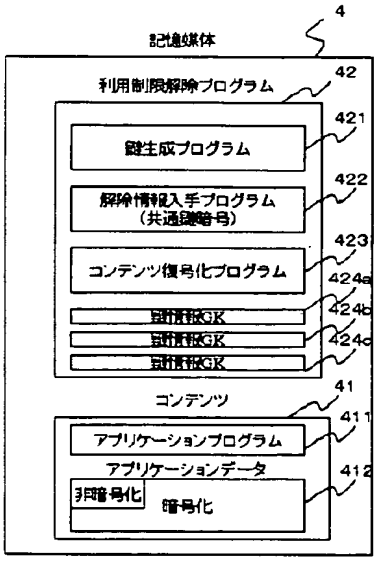
【図９】

図9



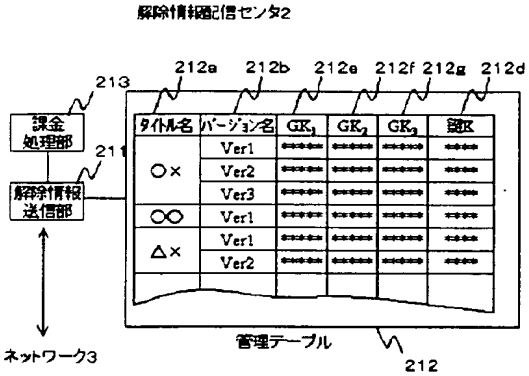
【図１０】

図10



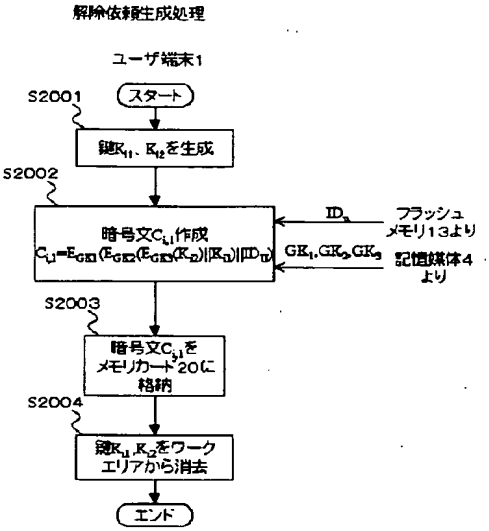
【図１１】

図11



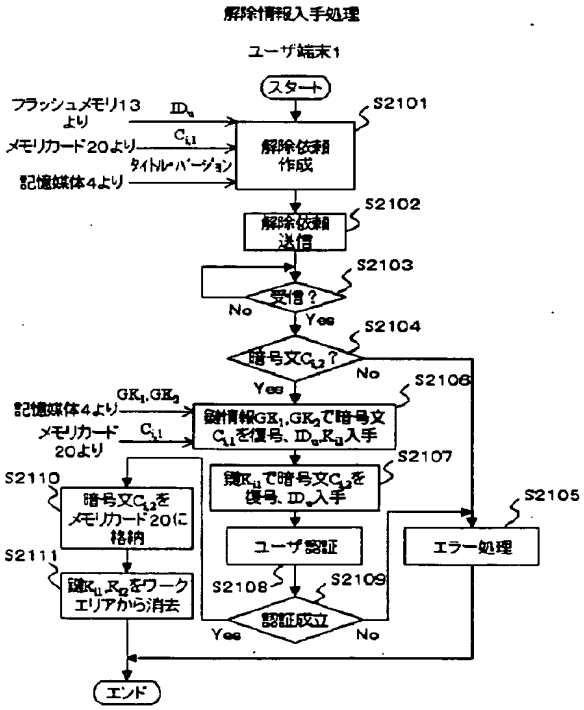
【図１２】

図12



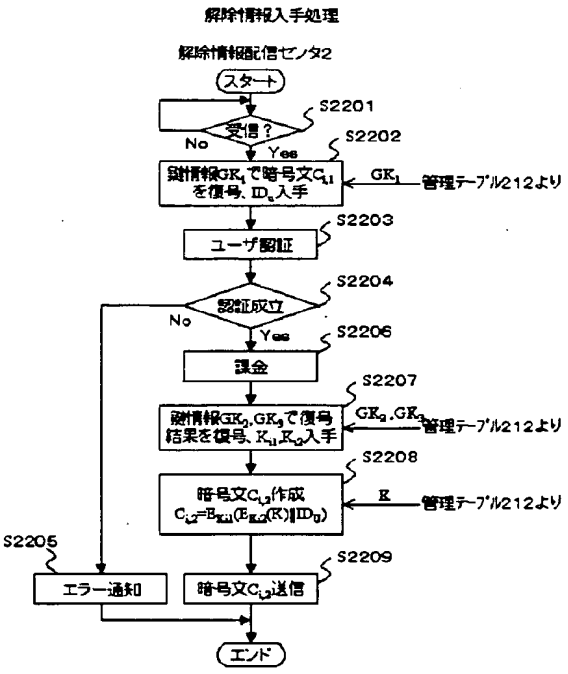
【図１３】

図13



【図１４】

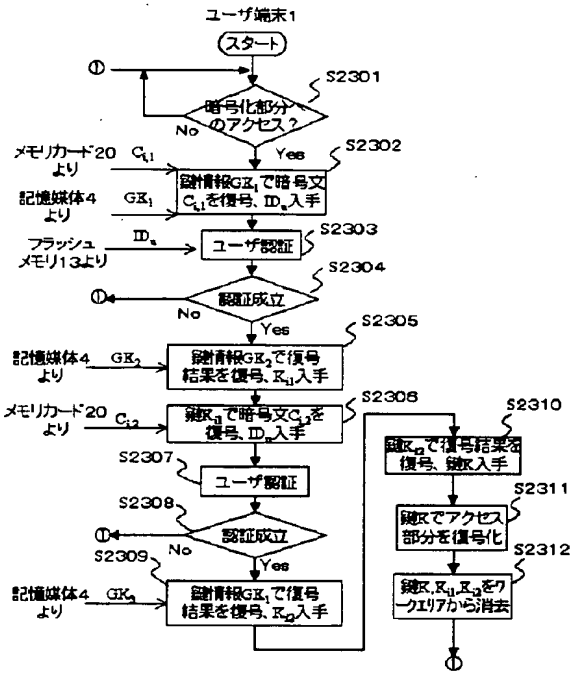
図14



【図１５】

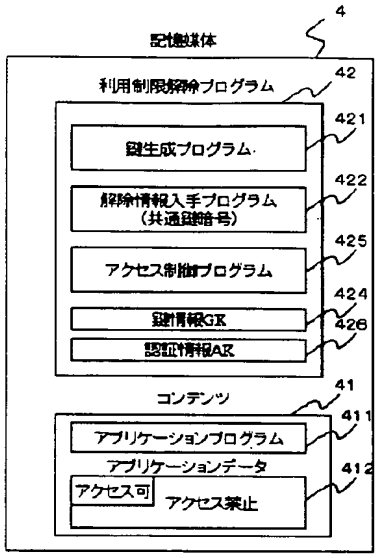
図15

コンテンツ復号化処理



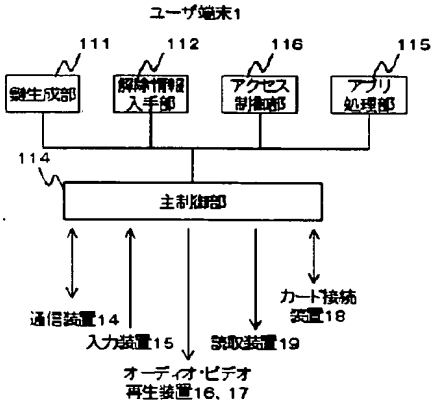
【図１６】

図16



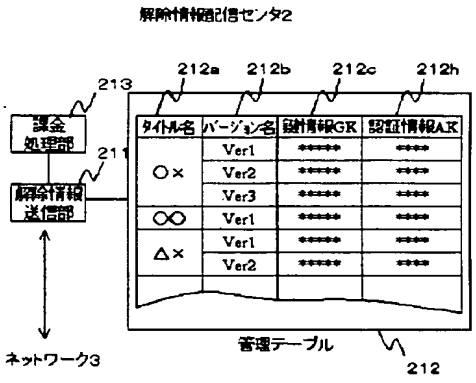
【図１７】

図17



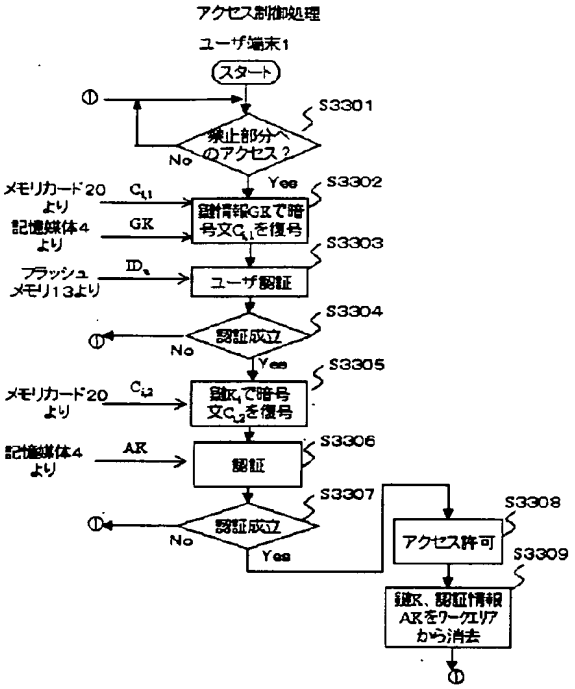
【図１８】

図18



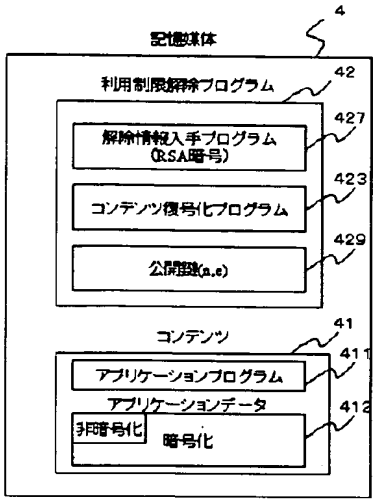
【図１９】

図19



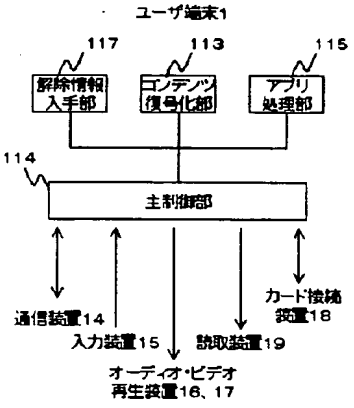
【図２０】

図20



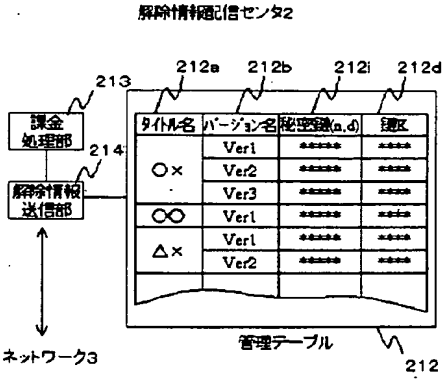
【図２１】

図21



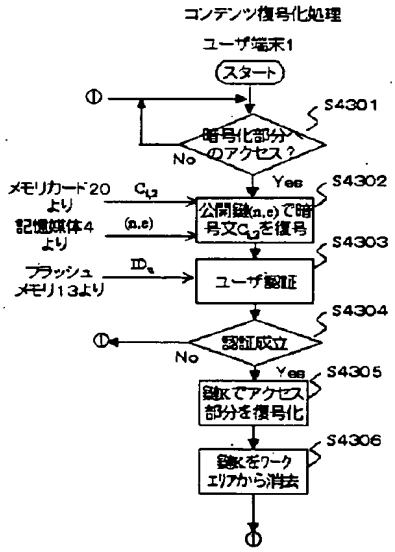
【図２２】

図22



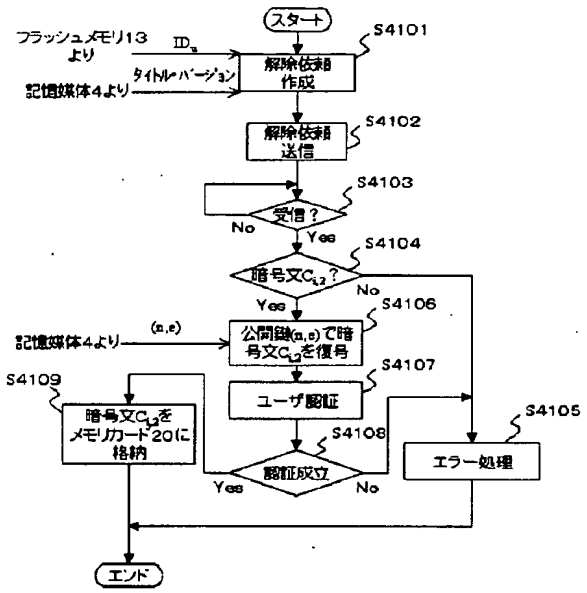
【図２５】

図25



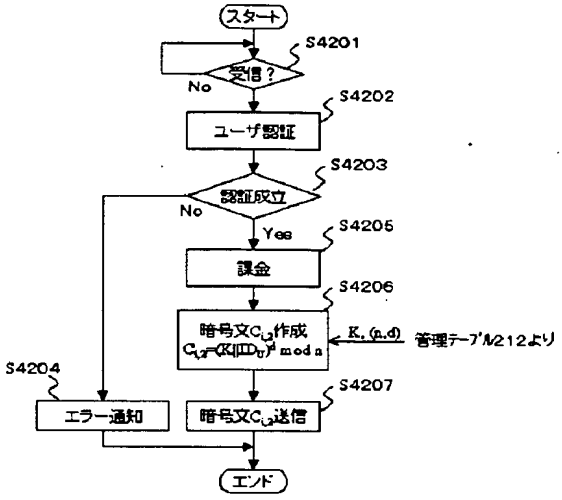
【図２３】

図23



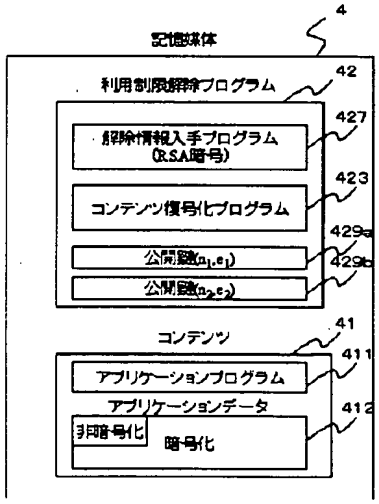
【図２４】

図24



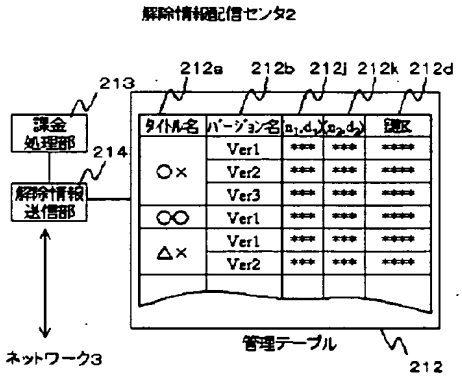
【図２６】

図26



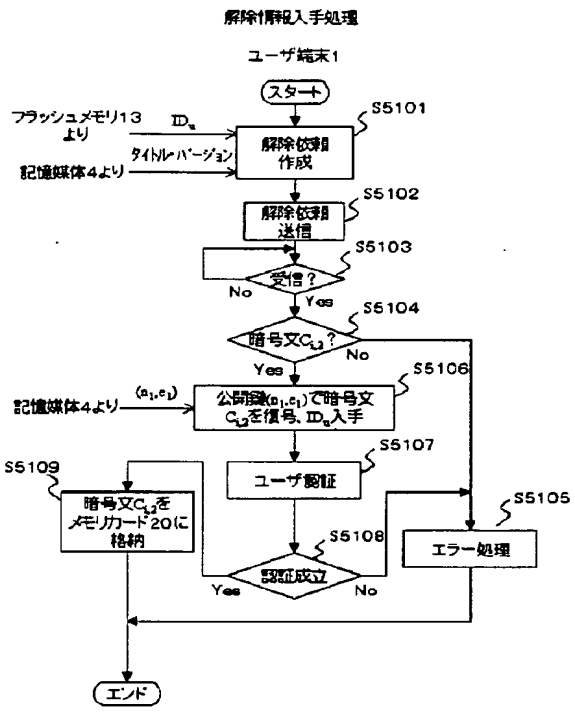
【図２７】

図27



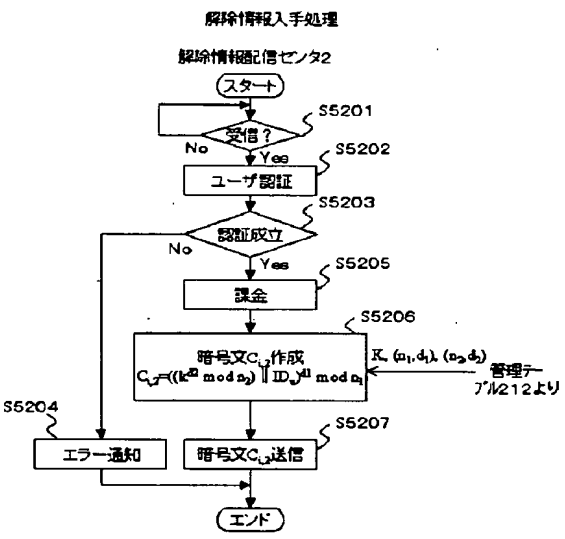
【図２８】

図28



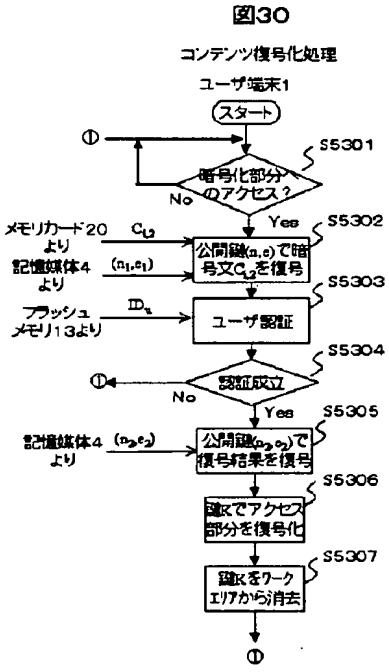
【図２９】

図29



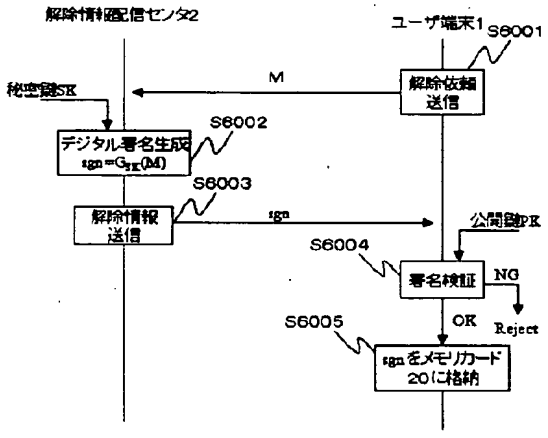
【図３０】

図30



【図３１】

図31



フロントページの続き

(51)Int.Cl.'	識別記号	F I		テーマコード（参考）
Ｈ０４Ｎ	5/85	Ｈ０４Ｌ	9/00	６２１Ａ
	5/91			６７３Ａ
	7/167			６７３Ｃ
		Ｈ０４Ｎ	5/91	Ｐ
			7/167	Ｚ

(72)発明者　瀬戸　洋一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　若林　隆
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所サービス事業部内
(72)発明者　鉄井　俊明
東京都小平市上水本町五丁目20番１号　株式会社日立製作所半導体グループ内
(72)発明者　山中　勇毅
東京都大田区羽田１丁目２番12号　株式会社セガ・エンタープライゼス内

Ｆターム(参考)　5B085 AA08 AE29
5C052 AA02 AB04 AB05 CC20 DD04
5C053 FA13 FA23 FA24 GB05 GB40 JA30 LA14
5C064 BA07 BB01 BB02 BC18 BD02 BD09 BD13
5J104 AA07 AA16 EA02 EA06 EA18 JA03 JA21 JA28 KA01 LA03 LA06 MA05 NA01 NA02 NA35 PA11